aws

Entwicklerhandbuch

Amazon Simple Email Service

Amazon Simple Email Service: Entwicklerhandbuch

Table of Contents

Was ist Amazon SES? ... 1
Vorteile ... 1
Zugehörige Services ... 1
Preisgestaltung ... 2
Regionen ... 2
SES-Regionen und Endpunkte ... 3
Sandbox- und Sendelimit-Erhöhungen ... 4
Verifizierung von E-Mail-Adressen und Domänen ... 4
Easy DKIM ... 5
Unterdrückungsliste auf Kontoebene ... 5
Feedback-Benachrichtigungen ... 5
SMTP-Anmeldeinformationen ... 6
Feedback-Endpunkte, die für benutzerdefinierte MAIL FROM-Domänen verwendet werden ... 6
Sendeautorisierung ... 7
Empfangen von E-Mails ... 7
Kontingente ... 7
E-Mail-Sendekontingente ... 7
Kontingente für den E-Mail-Empfang ... 11
Mail Manager-Kontingente ... 13
Allgemeine Kontingente ... 15
Arten der Anmeldeinformation ... 15
Funktionsweise von Amazon SES ... 21
Nachdem ein Sender eine E-Mail-Anforderung an SES sendet ... 22
Nachdem Amazon SES eine E-Mail gesendet hat ... 23
E-Mail-Format ... 25
Grundlegendes zu Lieferbarkeit ... 29
Bewährte Methoden für E-Mails ... 36
Arbeitet mit AWS SDKs ... 43
Erste Schritte ... 45
Einrichtung ... 45
Melde dich an für AWS ... 45
Einrichten Ihres SES-Kontos ... 46

Gewähren Sie programmatischen Zugriff (um außerhalb der Konsole mit SES zu interagieren) ... 46
Laden Sie ein AWS SDK herunter (zur Verwendung des SES APIs) ... 48
Migration zu Amazon SES ... 49
Schritt 1. Überprüfen Ihrer Domäne ... 49
Schritt 2. Anfordern von Produktionszugriff. ... 49
Schritt 3. Konfigurieren von Domänenauthentifizierungssystemen ... 49
Schritt 4. Erstellen Ihrer SMTP-Anmeldeinformationen ... 50
Schritt 5. Herstellen einer Verbindung mit einem SMTP-Endpunkt ... 50
Nächste Schritte ... 50
Anfordern von Produktionszugriff. ... 51
Sendelimits ... 55
Erhöhen Ihrer Sendekontingente ... 57
Automatisch erhöhte Sendekontingente ... 57
Benutzer angefordert erhöhte Sendequoten ... 58
Überwachung Ihrer Sendekontingente ... 59
Überwachung Ihrer Sendekontingente mithilfe der Amazon-SES-Konsole ... 59
Überwachung Ihrer Sendekontingente mithilfe der Amazon-SES-API ... 60
Sendekontingent-Fehler ... 61
Erreichen von Sendelimits mit der Amazon-SES-API ... 61
Erreichen von Sendelimits mit SMTP ... 61
Einrichten des E-Mail-Versand ... 63
Verwenden der SMTP-Schnittstelle ... 63
Anforderungen zum Senden von E-Mails über SMTP ... 64
Methoden zum Senden von E-Mails über SMTP ... 65
Anzugebende E-Mail-Informationen ... 65
Abrufen Ihrer SMTP-Anmeldeinformationen ... 66
Herstellen einer Verbindung mit einem SMTP-Endpunkt ... 75
Senden von E-Mails über mithilfe von Softwarepaketen ... 76
Programmgesteuertes Versand von E-Mails ... 78
Integrieren in Ihren vorhandenen E-Mail-Server ... 89
Testen Ihrer Amazon SES SMTP-Schnittstellenverbindung ... 103
Verwenden der API ... 112
Senden einer formatierten E-Mail ... 114
Senden von Raw-E-Mails ... 114
Verwenden von Vorlagen zum Senden von E-Mails ... 126

Senden von E-Mails mit einem AWS SDK ... 151
Inhaltskodierungen ... 171
Unterstützte Sicherheitsprotokolle ... 172
E-Mail-Absender an Amazon SES ... 172
Amazon SES an Empfänger ... 173
End-to-end Verschlüsselung ... 174
Unterstützte Header-Felder ... 174
E-Mail-Anhänge ... 177
Wie funktionieren Anlagen ... 178
Struktur des Anhangsobjekts ... 178
Best Practices ... 183
Nicht-unterstützte Anhangtypen ... 183
Empfangen von E-Mails ... 185
E-Mail-Empfangskonzepte & Anwendungsfälle ... 186
Empfängerbasierte Steuerung mit Zahlungsregeln ... 186
IP-basierte Steuerung mit IP-Adressfiltern ... 188
E-Mail-Empfangsprozess ... 189
Anwendungsfälle & Einschränkungen ... 190
E-Mail-Authentifizierung und Malware-Erkennung ... 193
Einrichten des E-Mail-Empfangs in ... 195
Verifizieren Ihrer Domäne ... 196
Veröffentlichen eines MX-Datensatzes ... 196
Erteilen von Berechtigungen ... 199
Exemplarische Vorgehensweisen für die E-Mail-Empfangskonsole ... 209
Erstellen von Empfangsregeln ... 209
Erstellen von IP-Filtern ... 252
Metriken zum E-Mail-Empfang ... 253
Mieter - NEU ... 257
Was ist Mieterverwaltung? ... 257
Funktionsweise ... 258
Zuordnung der Ressourcen ... 258
Reputationsüberwachung ... 258
Einrichtung ... 259
Mieter erstellen ... 259
Zuweisen von Ressourcen ... 260
Reputationsrichtlinien ... 261

Versand von E-Mails ... 262
SendEmail-API ... 262
SMTP ... 263
Status des Mieters ... 263
Status und Metriken ... 263
Pause/Pause beenden ... 264
Ergebnisse zur Reputation ... 265
Anzeigen von -Ergebnissen ... 265
Grundlegendes zu Erkenntnissen ... 266
Lösung von Problemen ... 267
Überwachen ... 267
CloudWatch Metriken ... 267
EventBridge-Benachrichtigungen ... 268
Vertrauen und Sicherheit ... 270
Best Practices ... 271
Einschränkungen ... 272
Preisgestaltung ... 273
Verifizierte Identitäten ... 274
Erstellen und Verifizieren von Identitäten ... 274
Erstellen einer Domänenidentität ... 278
Verifizieren einer Domänenidentität ... 282
Erstellen einer E-Mail-Adressidentität ... 288
Verifizieren der Identität einer E-Mail-Adresse ... 290
Erstellen und überprüfen Sie eine Identität und weisen Sie gleichzeitig eine Standardkonfiguration zu (API) ... 291
Verwenden von benutzerdefinierten Vorlagen zur E-Mail-Verifizierung ... 292
Verwalten der Identitäten ... 305
Identitäten mithilfe der Konsole anzeigen ... 305
Löschen Sie eine Identität mithilfe der Konsole ... 306
Bearbeiten Sie eine Identität mit der Konsole ... 307
Bearbeiten Sie eine Identität, um einen Standardkonfigurationssatz mithilfe der SES-API zu verwenden ... 308
Rufen Sie den von der Identität verwendeten Standardkonfigurationssatz mithilfe der SES-API ab ... 309
Überschreiben Sie den aktuellen Standardkonfigurationssatz, der von der Identität verwendet wird, mithilfe der SES-API ... 310

Konfigurieren von Identitäten ... 311
E-Mail-Authentifizierungsmethoden ... 311
Einrichten von Ereignisbenachrichtigungen ... 365
Verwenden der Identitätsautorisierung ... 407
Verwenden der Sendeautorisierung ... 423
Senden von Test-E-Mails mit dem Simulator ... 458
Verwenden des Postfachsimulators über die Konsole ... 458
Manuelles Verwenden des Postfachsimulators ... 460
Konfigurationssätze ... 465
Erstellen Sie einen Konfigurationssatz. ... 466
So erstellen Sie einen Konfigurationssatz ... 466
Konfigurationssatz erstellen (AWS CLI) ... 472
Verwalten von Konfigurationssätzen ... 474
Konfigurationssatz anzeigen, bearbeiten und löschen (Konsole) ... 474
Konfigurationssätze auflisten (AWS CLI) ... 475
Details zum Konfigurationssatz abrufen (AWS CLI) ... 475
Löschen eines Konfigurationssatzes (AWS CLI) ... 475
Beenden Sie das Senden von E-Mails aus einem Konfigurationssatz (AWS CLI) ... 475
Grundlegendes zu den Standardkonfigurationssätzen ... 476
Ereignisziele erstellen ... 477
IP-Pols zuweisen ... 483
Konfigurieren von benutzerdefinierten Domänen ... 484
Festlegen von Konfigurationssätzen für E-Mails ... 491
Reputationsmetriken anzeigen und exportieren ... 491
Aktivieren des Exports von Reputationsmetriken ... 492
Deaktivieren des Exports von Reputation-Metriken ... 492
Globale Endpunkte ... 493
Was sind globale Endgeräte? ... 493
So funktionieren globale Endgeräte ... 493
Einrichtung globaler Endpunkte ... 494
Voraussetzungen ... 494
Einen globalen Endpunkt erstellen ... 494
Globale Endpunktstaaten ... 495
Die sekundäre Region wird vorbereitet ... 496
(1) Doppelte Konfigurationssätze ... 496
(2) Doppelte verifizierte Domain-Identitäten ... 497

(3) Doppelte Produktionsgrenzen ... 498
Verwendung globaler Endpunkte ... 500
Integrieren in Ihre Anwendung ... 500
Überwachung und Metriken ... 501
Bewährte Methoden und Überlegungen ... 502
Preisgestaltung ... 502
Dedizierte IP-Adressen ... 503
Einfache Einrichtung ... 505
Reputationsverwaltung ... 505
Planbarkeit von Sendemustern ... 506
Volumen ausgehender E-Mails ... 507
Weitere Kosten ... 507
Kontrolle über die Senderzuverlässigkeit ... 507
Möglichkeit zur Isolierung der Senderzuverlässigkeit ... 508
Bekannte, unveränderliche IP-Adressen ... 508
Standard ... 508
Anfordern und Freigeben ... 509
Aufwärmen ... 511
Erstellen von Pools ... 515
Dedizierte IP-Adressen (verwaltet) ... 517
Vorteile und Funktionen ... 518
Bedeutung des Aufwärmens ... 520
Häufig gestellte Fragen, die Sie kennen sollten ... 521
Erstellen eines verwalteten IP-Pools ... 521
Anzeigen von Versand und Kapazität des Pools ... 525
Löschen eines verwalteten IP-Pools ... 527
Bring Your Own IP Addresses ... 528
Voraussetzungen ... 529
Überlegungen ... 529
Eigene IP-Adressen mit Amazon SES verwenden ... 530
Virtueller Zustellbarkeitsmanager ... 531
Erste Schritte ... 532
Erste Schritte (Konsole) ... 533
Erste Schritte (AWS CLI) ... 534
Dashboard ... 536
Verwenden des Dashboards (Konsole) ... 539

Zugreifen auf Metrikdaten (AWS CLI) ... 544
Filtern und Exportieren von Metrikdaten (AWS CLI) ... 545
Suchen nach Nachrichten, deren Status und Exportieren von Ergebnissen (AWS CLI) ... 546
Verwalten von Exportaufträgen (AWS CLI) ... 551
Anzeigen von Nachrichtendetails (AWS CLI) ... 553
So werden Dashboard-Metriken berechnet ... 553
Berater ... 556
Wonach sucht der Berater ... 558
Verwenden des Beraters (Konsole) ... 561
Zugriff auf Empfehlungen (AWS CLI) ... 562
Einstellungen ... 562
Ändern der Einstellungen des virtuellen Zustellbarkeitsmanages (optional) ... 563
Ändern der Einstellungen des virtuellen Zustellbarkeitsmanagers (AWS CLI) ... 564
E-Mail-Validierung ... 567
E-Mail-Validierungs-API ... 568
API-Validierung (Konsole) ... 569
API-Validierung (AWS CLI) ... 569
Automatische Validierung ... 572
Automatische Validierung (Konsole) ... 573
Überschreibungen von Konfigurationssätzen ... 574
Automatische Validierung (AWS CLI) ... 574
Dashboard zur E-Mail-Validierung ... 577
E-Mail-Manager ... 579
Erste Schritte ... 580
Erste Schritte ... 581
Eingangsendpunkte ... 582
Konfiguration von Eingangsendpunkten ... 583
TLS-Richtlinie ... 588
mTLS-Authentifizierung ... 590
Einen Ingress-Endpunkt (Konsole) erstellen ... 591
Verkehrspolitik und Grundsatzerklärungen ... 594
Erstellung von Verkehrsrichtlinien und Richtlinienerklärungen (Konsole) ... 596
Bedingungen der Grundsatzerklärung ... 597
Regelsätze und Regeln ... 599
Regelsätze und Regeln erstellen (Konsole) ... 600
Regelbedingungen und Aktionen ... 602

SMTP-Relais ... 607
Ein SMTP-Relay (Konsole) erstellen ... 609
Google Workspaces einrichten ... 613
Microsoft Office 365 einrichten ... 614
Adresslisten ... 617
Was sind Adresslisten? ... 618
Wie funktionieren Adresslisten ... 618
Adresslisten einrichten ... 618
Verwenden von Adresslisten ... 623
Bewährte Methoden ... 502
E-Mail-Archivierung ... 626
Verwenden der E-Mail-Archivierung (Konsole) ... 627
Fügen Sie Ons per E-Mail hinzu ... 632
Add Ons abonnieren (Konsole) ... 633
Berechtigungsrichtlinien ... 635
Richtlinien für Eingangsendpunkte ... 635
SMTP-Relay-Richtlinien ... 637
Richtlinien für die E-Mail-Archivierung ... 639
Richtlinien für Regelaktionen ... 643
Protokollierung ... 651
Einrichten der Protokollbereitstellung ... 651
Interpretieren der Protokolle ... 654
Abonnements auflisten ... 661
Globale Unterdrückungsliste ... 663
Überlegungen zur globalen Unterdrückungsliste ... 664
Verwenden der Unterdrückungsliste auf Kontoebene ... 665
Überlegungen zur Unterdrückungsliste auf Kontoebene ... 666
Aktivieren der Unterdrückungsliste auf Kontoebene ... 667
Aktivieren Ihrer Unterdrückungsliste auf Kontoebene für einen Konfigurationssatz ... 669
Hinzufügen einzelner E-Mail-Adressen zu Ihrer Unterdrückungsliste auf Kontoebene ... 671
Hinzufügen von E-Mail-Adressen in Ihrer Unterdrückungsliste auf Kontoebene ... 672
Anzeigen einer Liste der Adressen, die sich in Ihrer Unterdrückungsliste auf Kontoebene befinden ... 676
Löschen einzelner E-Mail-Adressen aus Ihrer Unterdrückungsliste auf Kontoebene ... 679
Löschen von E-Mail-Adressen aus Ihrer Unterdrückungsliste auf Kontoebene ... 680
Anzeigen einer Liste von Importaufträgen für das Konto ... 684

Abrufen von Informationen über einen Importauftrag für das Konto ... 686
Aktivieren der Unterdrückungsliste auf Kontoebene ... 687
Verwenden der Unterdrückung auf Konfigurationssatzebene ... 688
Aktiviereung der Unterdrückung auf Satzebene auf Konfigurationseinstellung ... 691
Verwenden von Listenverwaltung ... 692
Übersicht über die Verwaltung von ... 693
Konfigurieren der Listenverwaltung ... 693
Exemplarische Vorgehensweise zur Listenverwaltung mit Beispielen ... 699
Abonnementverwaltung ... 702
Abonnementverwaltung ... 702
Überlegungen zur Abmeldung von Kopfdaten ... 703
Hinzufügen eines Link zum Abmelden der Fußzeile ... 704
Überwachen der SMS-Aktivität ... 705
Überwachen mithilfe der Konsole ... 713
Konto-Dashboard ... 713
Zuverlässigkeitsmetriken ... 715
SMTP-Einstellungen ... 716
Verwenden der Konsole zum Überwachen von Metriken ... 717
Überwachen mithilfe der API ... 718
Aufrufen der `GetSendStatistics` API-Operation mit dem AWS CLI ... 719
Programmgesteuertes Aufrufen der Operation `GetSendStatistics` ... 720
Überwachen des E-Mail-Versands mithilfe der Ereignisveröffentlichung ... 723
So funktioniert die Veröffentlichung von Ereignissen mit Konfigurationssätzen und Nachrichten-Tags ... 724
Detailliertes Feedback für E-Mail-Kampagnen ... 725
Verwenden der Ereignisveröffentlichung ... 726
Terminologie zu Ereignisveröffentlichung ... 727
Einrichten der Ereignisveröffentlichung ... 728
Arbeiten mit Ereignisdaten ... 745
Überwachen Ihrer Absenderzuverlässigkeit ... 823
Verwenden von Reputation-Kennzahlen ... 823
Reputation Metriken Nachrichten ... 826
Allgemeine Statusnachrichten ... 826
Benachrichtigung zur Unzustellbarkeitsquote ... 828
Benachrichtigung zur Beschwerdequote ... 830
Benachrichtigungen zur Anti-Spam-Organisation ... 831

Listbombing-Benachrichtigung ... 833
Benachrichtigungen zu direktem Feedback ... 834
Domain-Blocklist-Benachrichtigungen ... 836
Benachrichtigung zur internen Überprüfung ... 837
Benachrichtigung zum E-Mail-Dienstanbieter ... 839
Benachrichtigung zu Empfänger-Feedback ... 840
Benachrichtigung zu verknüpftem Konto ... 842
Benachrichtigung zu Pseudo-E-Mail-Adressen für Spam ... 843
Benachrichtigung zur Websiteanfälligkeit ... 844
Benachrichtigung zu kompromittierten Anmeldeinformationen ... 846
Sonstige Benachrichtigung ... 847
Erstellen von Alarmen mithilfe von CloudWatch ... 847
SNDS-Metriken für dedizierte IPs ... 850
Vorschläge für die Fehlerbehebung ... 852
Automatisches Unterbrechen des E-Mail-Versands ... 853
Für Ihr gesamtes Konto ... 853
Für einen Konfigurationssatz ... 861
Überwachung mit EventBridge ... 871
SES-Ereignisse ... 871
Referenz zu Ereignisschemas ... 873
Schema des Status des Virtual-Deliverability-Manager-Beraters ... 874
Statusschema für den SES-E-Mail-Versand ... 876
Verwenden EventBridge ... 878
Geben Sie ein Beispielereignis an in EventBridge ... 879
Ereignismuster für SES-Ereignisse ... 879
Zusätzliche EventBridge Ressourcen ... 882
Codebeispiele ... 883
Amazon SES ... 885
Grundlagen ... 887
Szenarien ... 1019
Amazon SES API v2 ... 1068
Grundlagen ... 1069
Szenarien ... 1135
Sicherheit ... 1177
Datenschutz ... 1178
Verschlüsselung von Daten im Ruhezustand ... 1179

Verschlüsselung während der Übertragung ... 1192
Löschen personenbezogener Daten ... 1192
Identity and Access Management ... 1199
Erstellen von IAM-Richtlinien für den Zugriff auf SES ... 1200
Beispiel-IAM-Richtlinien für SES ... 1204
AWS verwaltete Richtlinien ... 1210
Verwenden von servicegebundenen Rollen ... 1213
Protokollierung und Überwachung ... 1216
Protokollieren von API-Aufrufen ... 1216
Compliance-Validierung ... 1228
Ausfallsicherheit ... 1229
Infrastruktursicherheit in SES ... 1229
VPC-Endpunkte ... 1229
Anleitungsbeispiel für die Einrichtung von SES in Amazon VPC ... 1230
Fehlerbehebung ... 1235
Allgemeine Probleme ... 1236
Änderungen, die ich vornehme, sind nicht direkt sichtbar ... 1236
Verifizierungsprobleme ... 1237
Probleme mit der Domänenverifizierung ... 1237
Überprüfen der Einstellungen für die Domänenverifizierung ... 1239
Probleme bei der E-Mail-Verifizierung ... 1241
DKIM-Probleme ... 1241
Zustellungsprobleme ... 1244
Probleme mit empfangenen E-Mails ... 1245
Benachrichtigungsprobleme ... 1246
Fehler beim Senden von E-Mails ... 1247
Erhöhen des -Durchsatzes ... 1250
SMTP-Probleme ... 1252
SMTP-Antwortcodes ... 1254
FAQs ... 1262
Verwaltetes DIPS FAQs ... 1262
Häufig gestellte Fragen zu verwalteten DIPS Q1 ... 1262
Häufig gestellte Fragen zu verwalteten DIPS, Q2 ... 1263
Häufig gestellte Fragen zu verwalteten DIPS, Q3 ... 1263
Häufig gestellte Fragen zu verwalteten DIPS, Q4 ... 1263
Häufig gestellte Fragen zu verwalteten DIPS Q5 ... 1264

Häufig gestellte Fragen zu verwalteten DIPS Q6 1264
Überprüfungsprozess für den Versand FAQs 1264
Konto wird geprüft 1265
Sendeunterbrechungen 1268
Unzustellbarkeit 1272
Complaints (Beschwerden) 1276
Pseudo-E-Mail-Adressen für Spam 1283
Manuelle Überprüfungen 1286
DNS-Blackhole-Liste (DNSBL) FAQs 1288
DNSBL FAQ Q1 1289
DNSBL FAQ Q2 1289
DNSBL FAQ Q3 1290
DNSBL FAQ Q4 1290
DNSBL FAQ Q5 1291
DNSBL FAQ Q6 1292
E-Mail-Metriken FAQs 1293
General 1294
Öffnungsnachverfolgung 1295
Klicknachverfolgung 1296
Schnellsuchindex 1300
Anleitungen und Konzepte 1300
..... mcccvii

Was ist Amazon SES?

Amazon Simple Email Service (SES) ist eine E-Mail-Plattform, die Ihnen eine einfache und kostengünstige Möglichkeit bietet, E-Mails mit Ihren eigenen E-Mail-Adressen und Domains zu versenden und zu empfangen.

Sie können beispielsweise Marketing-E-Mails wie Sonderangebote, Transaktions-E-Mails wie Auftragsbestätigungen und andere Korrespondenzarten wie Newsletter senden. Wenn Sie Amazon SES verwenden, um E-Mails zu empfangen, können Sie Softwarelösungen wie E-Mail-Autoresponder, E-Mail-Abmeldesysteme und Anwendungen entwickeln, die Kundensupport-Tickets aus eingehenden E-Mails generieren.

Weitere Informationen zu Amazon SES -Themen finden Sie imAWS Blog für Messaging und Targeting.

Vorteile

Die Einrichtung einer großdimensionierten E-Mail-Lösung ist oft eine komplexe und kostenintensive Herausforderung für ein Unternehmen. Sie müssen sich mit Infrastrukturproblemen, z. B. Mailserververwaltung, Netzwerkkonfiguration und IP-Adressenzuverlässigkeit, auseinandersetzen. Darüber hinaus kommen für viele E-Mail-Lösungen von Drittanbietern Vertrags- und Preisverhandlungen hinzu sowie erhebliche Vorinvestitionen. Amazon SES beseitigt diese Herausforderungen und ermöglicht Ihnen, von der jahrelangen Erfahrung und hochwertigen E-Mail-Infrastruktur, die Amazon.com für seinen eigenen umfangreichen Kundenstamm aufgebaut hat, zu profitieren.

Zugehörige Services

Amazon SES lässt sich nahtlos in andere AWS Produkte integrieren. Beispielsweise ist Folgendes möglich:

- Fähigkeiten zum Versenden von E-Mails zu jeder beliebigen Anwendung hinzufügen.
- Sie können E-Mails von Amazon senden, EC2 indem Sie ein AWS SDK verwenden, die Amazon SES SMTP-Schnittstelle verwenden oder indem Sie direkt die Amazon SES SES-API aufrufen.
- Verwenden Sie AWS Elastic Beanstalk, um eine E-Mail-fähige Anwendung zu erstellen – z. B. ein Programm, das mithilfe von Amazon SES einen Newsletter an Kunden versendet.

- Richten Sie Amazon Simple Notification Service (Amazon SNS) ein, um Sie über Ihre E-Mails zu informieren, die zurückgewiesen worden sind, eine Beschwerde hervorgerufen haben oder erfolgreich an den Mailserver des Empfängers zugestellt wurden. Wenn Sie Amazon SES verwenden, um E-Mails zu empfangen, können Ihre E-Mail-Inhalte in Amazon SNS-Themen veröffentlicht werden.
- Verwenden Sie das AWS-Managementkonsole , um Easy DKIM einzurichten, mit dem Sie Ihre E-Mails authentifizieren können. Obwohl Sie Easy DKIM mit jedem DNS-Provider verwenden können, ist es besonders einfach einzurichten, wenn Sie Ihre Domäne mit Route 53 verwalten.
- Steuern Sie den Benutzerzugriff auf den E-Mail-Versand mit Hilfe von AWS Identity and Access Management (IAM).
- Speichern Sie empfangene E-Mails in Amazon Simple Storage Service (Amazon S3)aus.
- Führen Sie über das Auslösen von AWS Lambda-Funktionen Aktionen für empfangene E-Mails aus.
- Verwenden Sie AWS Key Management Service (AWS KMS), um optional die E-Mails zu verschlüsseln, die Sie in Ihrem Amazon S3-Bucket erhalten.
- Verwenden Sie AWS CloudTrail, um Amazon SES-API-Aufrufe zu protokollieren, die Sie über die Konsole oder die Amazon-SES API durchführen.
- Veröffentlichen Sie Ihre E-Mail-Sendeereignisse bei Amazon CloudWatch oder Amazon Data Firehose. Wenn Sie Ihre E-Mail-Sendeereignisse in Firehose veröffentlichen, können Sie in Amazon Redshift, Amazon OpenSearch Service oder Amazon S3 darauf zugreifen.

Preisgestaltung

Mit Amazon SES zahlen Sie basierend auf der Menge der gesendeten und empfangenen E-Mails. Weitere Informationen finden Sie unter Amazon SES – Preise.

Regionen und Amazon SES

SES ist in mehreren Ländern AWS-Regionen auf der ganzen Welt erhältlich. AWS Unterhält in jeder Region mehrere Availability Zones. Diese Availability Zones sind physisch voneinander isoliert, jedoch durch private, hochredundante Netzwerkverbindungen mit geringer Latenz und hohem Durchsatz miteinander verbunden. Mithilfe dieser Availability Zones können wir ein sehr hohes Maß an Verfügbarkeit und Redundanz bieten und dabei gleichzeitig die Latenz minimieren.

Eine Liste aller regionalen SES-Endpunkte finden Sie unter Amazon Simple Email Service-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz Weitere Informationen zur Anzahl der Availability Zones, die in jeder Region verfügbar sind, finden Sie unter AWS Globale Infrastruktur.

Dieser Abschnitt enthält Informationen, die Sie benötigen, wenn Sie SES in mehreren Fällen verwenden möchten AWS-Regionen. Es werden die folgenden Themen behandelt:

- SES-Regionen und Endpunkte
- Sandbox- und Sendelimit-Erhöhungen
- Verifizierung von E-Mail-Adressen und Domänen
- Easy DKIM
- Unterdrückungsliste auf Kontoebene
- Feedback-Benachrichtigungen
- SMTP-Anmeldeinformationen
- Sendeautorisierung
- Feedback-Endpunkte, die für benutzerdefinierte MAIL FROM-Domänen verwendet werden
- Empfangen von E-Mails
- Einrichten von (MX-)Datensätzen

Allgemeine Informationen dazu AWS-Regionen finden Sie unter AWS Service-Endpunkte in der AWS Allgemeinen Referenz.

SES-Regionen und Endpunkte

Wenn Sie SES zum Senden von E-Mails verwenden, stellen Sie eine Verbindung zu einer URL her, die einen Endpunkt für die SES-API oder SMTP-Schnittstelle bereitstellt. Die Allgemeine AWS-Referenzenthält eine vollständige Liste der Endpunkte, die Sie zum Senden und Empfangen von E-Mails über SES verwenden. Weitere Informationen finden Sie unter Endpunkte und Kontingente von Amazon Simple Email Service Allgemeine AWS-Referenz in den folgenden spezifischen Abschnitten:

- API-Endpunkte — Wenn Sie E-Mails über SES senden, können Sie die in dieser Tabelle URLs aufgeführten Methoden verwenden, um HTTPS-Anfragen an die SES-API zu stellen.
- SMTP-Endpunkte — Sie können die in dieser Tabelle URLs aufgeführten Endpunkte verwenden, um E-Mails zu senden, wenn Sie die SMTP-Schnittstelle verwenden.

- E-Mail-Empfangsendpunkte — Wenn Sie SES für den Empfang von E-Mails konfiguriert haben, die an Ihre Domain gesendet wurden, können Sie den in dieser Tabelle URLs aufgeführten SMTP-Endpunkt für eingehende E-Mails verwenden, wenn Sie die Mail Exchanger (MX) -Einträge in den DNS-Einstellungen für Ihre Domain einrichten.

> **Note**
>
> Die eingehenden SMTP-Nachrichten URLs sind keine IMAP-Serveradressen. Mit anderen Worten: Sie können auf diese Weise keine E-Mails über eine Anwendung wie Outlook empfangen. Einen Service, der einen IMAP-Server für eingehende E-Mails bereitstellt, finden Sie auf Amazon WorkMail.

Sandbox- und Sendelimit-Erhöhungen

Der Sandbox-Status für Ihr Konto kann sich zwischen diesen unterscheiden. AWS-Regionen Mit anderen Worten, wenn Ihr Konto aus der Sandbox in der Region USA West (Oregon) entfernt wurde, befindet es sich möglicherweise immer noch in der Sandbox in der Region USA Ost (Nord-Virginia), es sei denn, Sie haben es auch aus der Sandbox in dieser Region entfernt.

Die Sendelimits können je nach auch unterschiedlich sein. AWS-Region Wenn Ihr Konto beispielsweise in der Region Europa (Irland) 10 Nachrichten pro Sekunde senden kann, können Sie in anderen Regionen möglicherweise mehr oder weniger Nachrichten senden.

Wenn Sie eine Anfrage einreichen, um Ihr Konto aus der Sandbox zu entfernen, oder wenn Sie eine Anfrage zur Erhöhung der Sendekontingente Ihres Kontos einreichen, achten Sie darauf, alle Felder auszuwählen, auf AWS-Regionen die sich Ihre Anfrage bezieht. Sie können in einem einzelnen Supportcenter-Fall mehrere Anfragen senden.

Verifizierung von E-Mail-Adressen und Domänen

Bevor Sie E-Mails mit SES versenden können, müssen Sie verifizieren, dass Sie Eigentümer der E-Mail-Adresse oder Domain sind, von der aus Sie versenden möchten. Der Bestätigungsstatus von E-Mail-Adressen und Domains ist ebenfalls von Land zu Land unterschiedlich AWS-Regionen. Wenn Sie beispielsweise eine Domain in der Region USA West (Oregon) verifizieren, können Sie diese Domain nicht zum Senden von E-Mails in der Region USA Ost (Nord-Virginia) verwenden, bis Sie den Bestätigungsprozess für diese Region erneut abgeschlossen haben. Weitere Informationen zur

Verifizierung von E-Mail-Adressen und Domänen finden Sie unter Verifizierte Identitäten in Amazon SES.

Easy DKIM

Sie müssen den Easy DKIM-Einrichtungsprozess für jeden Standort durchführen, AWS-Region in dem Sie Easy DKIM verwenden möchten. Das heißt, in jeder Region müssen Sie die SES-Konsole oder die SES-API verwenden, um CNAME-Einträge zu generieren. Als Nächstes müssen Sie alle CNAME-Einträge zur DNS-Konfiguration für Ihre Domain hinzufügen. Weitere Informationen zum Einrichten von Easy DKIM finden Sie unter Easy DKIM in Amazon SES.

Nicht alle AWS-Regionen verwenden die standardmäßige SES-DKIM-Domain. `dkim.amazonses.com` Um zu sehen, ob Ihre Region eine regionsspezifische DKIM-Domain verwendet, überprüfen Sie die Tabelle mit den DKIM-Domänen im. Allgemeine AWS-Referenz

Unterdrückungsliste auf Kontoebene

Ihre Liste zur Sperrung auf SES-Kontoebene gilt derzeit nur für Sie. AWS-Konto AWS-Region Mit SES API v2 oder der Konsole können Sie Adressen einzeln oder in Massen manuell zu Ihrer Unterdrückungsliste auf Kontoebene hinzufügen oder daraus entfernen. Weitere Hinweise zur Verwendung Ihrer Unterdrückungsliste auf Kontoebene finden Sie unter Verwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole.

Feedback-Benachrichtigungen

Bei der Einrichtung mehrerer Feedback-Benachrichtigungen sind zwei wichtige Punkte zu beachten: AWS-Regionen

- Einstellungen für verifizierte Identitäten, z. B. ob Sie Feedback per E-Mail oder über SNS erhalten, gelten nur für die Region, in der Sie sie eingerichtet haben. Wenn Sie beispielsweise user@example.com in den Regionen USA West (Oregon) und USA Ost (Nord-Virginia) verifizieren und zurückgesendete E-Mails über SNS-Benachrichtigungen erhalten möchten, müssen Sie die SES-API oder die SES-Konsole verwenden, um SNS-Feedback-Benachrichtigungen für user@example.com in beiden Regionen einzurichten.
- SNS-Themen, die Sie für die Feedback-Weiterleitung verwenden, müssen sich in derselben Region befinden, in der Sie SES verwenden.

Weitere Informationen zur Überwachung Ihrer Sendeaktivitäten durch Feedback-Benachrichtigungen finden Sie unterEinrichten von Ereignisbenachrichtigungen für Amazon SES.

SMTP-Anmeldeinformationen

Die Anmeldeinformationen, die Sie zum Senden von E-Mails über die SES SMTP-Schnittstelle verwenden, sind jeweils AWS-Region einzigartig. Wenn Sie die SES-SMTP-Schnittstelle zum Senden von E-Mails in mehr als einer Region verwenden, müssen Sie für jede Region einen Satz von SMTP-Anmeldeinformationen generieren.

> **Note**
>
> Wenn Sie Ihre SMTP-Anmeldeinformationen vor dem 10. Januar 2019 erstellt haben, wurden Ihre SMTP-Anmeldeinformationen mit einer älteren Version der Signatur erstellt. AWS Aus Sicherheitsgründen sollten Sie Anmeldeinformationen, die Sie vor diesem Datum erstellt haben, löschen und durch neue Anmeldeinformationen ersetzen. Sie können ältere Anmeldeinformationen mit der IAM-Konsole löschen.

Feedback-Endpunkte, die für benutzerdefinierte MAIL FROM-Domänen verwendet werden

Wenn Sie eine benutzerdefinierte MAIL FROM-Domain verwenden, verlangt SES von Ihnen, dass Sie einen MX-Eintrag veröffentlichen, damit Ihre Domain die Bounce- und Beschwerdebenachrichtigungen erhalten kann, die Ihnen E-Mail-Anbieter senden. Sie können dieselbe benutzerdefinierte MAIL FROM-Domain für verifizierte Identitäten auf unterschiedliche Weise verwenden, AWS-Regionen da die Absenz- und Beschwerdebenachrichtigungen an einen regionsspezifischen Feedback-Endpunkt gesendet werden.

Wenn Sie eine benutzerdefinierte MAIL FROM-Domäne konfigurieren, gibt SES automatisch den richtigen Feedback-Endpunkt für die Region an, in der das benutzerdefinierte MAIL FROM konfiguriert wird. Dieser Endpunkt wird im Wertfeld des MX-Eintrags bereitgestellt, sodass Sie ihn zur DNS-Konfiguration Ihrer Domain veröffentlichen (hinzufügen) können.

Der benutzerdefinierte MAIL FROM Einrichtungsvorgang ist in Verwenden einer benutzerdefinierten MAIL FROM-Domäne beschrieben. Als Referenz sind die Feedback-Endpunkte, die SES für die verschiedenen AWS-Regionen Feedback-Endpunkte verwendet, in der Tabelle mit den Feedback-Endpunkten im aufgeführt. Allgemeine AWS-Referenz

Sendeautorisierung

Delegierte Absender können E-Mails nur von dem Ort aus versenden, an AWS-Region dem die Identität des Identitätsinhabers verifiziert wurde. Die Richtlinie für die Sendeautorisierung, die dem stellvertretenden Sender seine Berechtigung erteilt, muss der Identität in dieser Region angefügt sein. Weitere Informationen zur Sendeautorisierung finden Sie unter Verwenden der Sendeautorisierung mit Amazon SES.

Empfangen von E-Mails

Mit Ausnahme von Amazon S3 S3-Buckets müssen sich alle AWS Ressourcen, die Sie für den Empfang von E-Mails mit SES verwenden, auf demselben AWS-Region wie der SES-Endpunkt befinden. Wenn Sie beispielsweise SES in der Region USA West (Oregon) verwenden, müssen sich alle SNS-Themen, KMS-Schlüssel und Lambda-Funktionen, die Sie verwenden, auch in der Region USA West (Oregon) befinden. Ebenso müssen Sie für den Empfang von E-Mails mit SES innerhalb einer Region einen aktiven Empfangsregelsatz in dieser Region erstellen. Die Konzepte und der Einrichtungsprozess für den E-Mail-Empfang werden unter erklärtEmpfang von E-Mails mit Amazon SES.

In der Tabelle mit den E-Mail-Empfangsendpunkten in der Allgemeine AWS-Referenz Tabelle sind die E-Mail-Empfangsendpunkte für alle Bereiche aufgeführt, AWS-Regionen in denen SES den E-Mail-Empfang unterstützt.

Servicekontingente in Amazon SES

In den folgenden Abschnitten werden die Kontingente aufgeführt und beschrieben, die für Amazon SES-Ressourcen und -Vorgänge gelten. Einige Kontingente können erhöht werden, andere dagegen nicht. Informationen dazu, ob Sie eine Erhöhung für ein Kontingent beantragen können, finden Sie in der Spalte Adjustable (Anpassbar).

> **Note**
>
> SES-Kontingente gelten für jedes AWS-Region , das Sie in Ihrem verwenden. AWS-Konto

E-Mail-Sendekontingente

Die folgenden Kontingente gelten für das Senden von E-Mails über SES.

Sendequote

Die Kontingente basieren auf der Anzahl der Empfänger und nicht auf der Anzahl der Nachrichten.

Ressource	Standardkontingent	Einstellbar
Anzahl der E-Mails, die innerhalb von 24 Stunden gesendet werden können	Wenn sich Ihr Konto in der Sandbox befindet, können Sie bis zu 200 E-Mails pro 24-Stunden-Zeitraum versenden. Befindet sich Ihr Konto nicht mehr in der Sandbox, variiert diese Zahl basierend auf Ihrem speziellen Anwendung sfall.	Yes (Ja)
Anzahl der E-Mails, die pro Sekunde gesendet werden können (Senderate)	Wenn sich Ihr Konto in der Sandbox befindet, können Sie 1 E-Mail pro Sekunde senden. Befindet sich Ihr Konto nicht mehr in der Sandbox, variiert diese Rate basierend auf Ihrem speziellen Anwendung sfall.	Yes (Ja)

Nachrichtenkontingente

Ressource	Standardkontingent	Einstellbar
Verwendung der maximalen SES v1-Nachrichtengröße (einschließlich Anhängen)	10 MB pro Nachricht (nach Base64-Kodierung).	Nein (Bei Workloads mit Nachrichtengrößen von mehr als 10 MB sollten Sie eine Migration auf die SES v2 in Erwägung ziehen.)

Ressource	Standardkontingent	Einstellbar
Verwendung der maximalen SES v2 oder SMTP-Nachrichtengröße (einschließlich Anhängen)	40 MB pro Nachricht (nach Base64-Kodierung).	Nein

> **Note**
>
> Nachrichten, die größer als 10 MB sind, unterliegen einer Bandbreitendrosselung, und abhängig von Ihrer Senderate werden Sie möglicherweise auf bis zu 40 MB/s gedrosselt. Sie könnten beispielsweise eine 40-MB-Nachricht mit einer Geschwindigkeit von 1 Nachricht pro Sekunde oder zwei 20 MB Nachrichten pro Sekunde senden.

Kontingente für Sender und Empfänger

Ressource	Standardkontingent	Einstellbar
Maximale Anzahl von Mietern	10.000	Ja
Maximale Anzahl von Empfängern pro Nachricht	50 Empfänger pro Nachricht. **Note** Ein Empfänger ist eine beliebige „An“-, „CC“- oder „BCC“-Adresse.	Nein.
Maximale Anzahl der Identitäten, die Sie verifizieren können	10.000 Identitäten pro. AWS-Region **Note** Eine Identität ist eine Domain oder E-Mail-Adresse, die Sie	Bitte wenden Sie sich an Ihren AWS Account Manager, um Ihren Anwendungsfall zu besprechen.

Ressource	Standardkontingent	Einstellbar
	verwenden, um E-Mails über SES zu versenden.	
Maximale Anzahl dedizierter IP-Pools (einschließlich verwalteter und standardmäßiger IP-Pools)	50	Nein

Kontingente für die Ereignisveröffentlichung

Ressource	Standardkontingent	Einstellbar
Maximale Anzahl von Konfigurationssätzen	10.000	Nein
Maximale Länge von Konfigurationssatz-Namen	Konfigurationssatz-Namen dürfen maximal 64 alphanumerische Zeichen enthalten. Sie dürfen auch Bindestriche (-) und Unterstriche (_) aufweisen. Namen dürfen keine Leerzeichen, Akzentbuchstaben oder andere Sonderzeichen enthalten.	Nein
Maximale Anzahl von Ereigniszielen pro Konfigurationssatz	10	Nein
Maximale Anzahl von Dimensionen pro CloudWatch Veranstaltungsziel	10	Nein

Kontingente für E-Mail-Vorlagen

Ressource	Standardkontingent	Einstellbar
Maximale Anzahl von E-Mail-Vorlagen in jeder AWS-Region	20 000	Nein
Maximale Vorlagengröße	500 KB	Nein
Maximale Anzahl von Ersatzwerten in jeder Vorlage	Unbegrenzt	–
Maximale Anzahl von Empfängern pro E-Mail-Vorlage	50 Zieladressen. Eine Zieladresse ist eine E-Mail-Adresse an „An“-, „CC“- oder „BCC“-Zeilen. **Note** Die Anzahl der Zieladressen, die Sie in einem einzigen Aufruf der API kontaktieren können, kann auf die maximale Senderate Ihres Kontos beschränkt sein.	Nein

Kontingente für den E-Mail-Empfang

In der folgenden Tabelle sind die Kontingente aufgeführt, die mit dem Empfang von E-Mails über SES verbunden sind.

Ressource	Standardkontingent	Einstellbar
Maximale Anzahl von Regeln pro Empfangsregelsatz	200	Nein
Maximale Anzahl von Aktionen pro Empfangsregel	10	Nein
Maximale Anzahl von Empfängern pro Empfangsregel	500	Nein
Maximale Anzahl von Empfangsregelsätzen pro AWS-Konto	40	Nein
Maximale Anzahl von IP-Adressfiltern pro AWS-Konto	100	Nein
Maximale E-Mail-Größe (einschließlich Header), die in einem Amazon-S3-Bucket gespeichert werden kann.	40 MB	Nein
Maximale E-Mail-Größe (einschließlich Header), die mit einer Amazon-SNS-Benachrichtigung veröffentlicht werden kann.	150 KB	Nein
Maximale Größe von E-Mail-Headern, die mit einer Amazon SNS SNS-Benachrichtigung veröffentlicht werden können	10 KB	Nein
Maximale Größe von E-Mail-Headern, die mit einer	50 KB	Nein

Ressource	Standardkontingent	Einstellbar
Funktion veröffentlicht werden können AWS Lambda		

Mail Manager-Kontingente

In der folgenden Tabelle sind die mit Mail Manager verbundenen Kontingente aufgeführt.

Ressource	Standardkontingent	Einstellbar
Maximale Anzahl offener Eingangsendpunkte	10	Nein
Maximale Anzahl autorisierter Eingangsendpunkte	50	Nein
Maximale Anzahl von Empfängern pro Nachricht	100	Nein
Maximale E-Mail-Größe (einschließlich Header)	40 MB	Nein
Maximale Anzahl von Aussagen zur Verkehrspolitik	20	Nein
Höchstzahl der Bedingungen für verkehrspolitische Erklärungen	10	Nein
Maximale Anzahl von Verkehrspolitiken pro Region	100	Nein
Maximale Anzahl von SMTP-Relays	40	Nein
Maximale Anzahl von Adresslisten pro Region	100	Nein

Ressource	Standardkontingent	Einstellbar
Maximale Anzahl von Adressen pro Adressliste	100 000	Nein
Maximale Anzahl von Regelsätzen	40	Nein
Maximale Anzahl von Regeln pro Regelsatz	40	Nein
Maximale Anzahl von Bedingungen pro Regel	10	Nein
Maximale Anzahl von Aktionen pro Regel	10	Nein
Maximale Anzahl von Relay- oder Sendeaktionen pro Regelsatz	10	Nein
Maximale Anzahl aktiver Archive	10	Nein
Maximale Anzahl von Archiv-Suchergebnissen	1000	Nein
Maximale Anzahl exportierter Archivsuchergebnisse	250 000	Nein
Maximale Anzahl laufender Suchanfragen parallel	1	Nein
Maximale Anzahl laufender Exportanfragen parallel	1	Nein
Maximale Anzahl von Aufbewahrungsänderungen für das Archiv pro Woche	1	Nein

Allgemeine Kontingente

In der folgenden Tabelle sind die Kontingente aufgeführt, die sowohl für das Senden als auch für das Empfangen von E-Mails über SES gelten.

Versandquoten für die SES-API

Ressource	Standardkontingent	Einstellbar
Rate, mit der Sie Amazon SES-API-Aktionen aufrufen können.	Alle Aktionen (mit Ausnahme von `SendEmail` , `SendRawEmail` und `SendTemplatedEmail`) werden auf eine Anforderung pro Sekunde gedrosselt.	Nein
MIME-Teile	500	Nein

Verschiedene SES-Kontingente

Ressource	Standardkontingent	Einstellbar
Maximale Anzahl gleichzeitiger Importaufträge	20	Nein
Maximale Anzahl gleichzeitiger Exportaufträge	20	Nein

Arten von Amazon-SES-Anmeldeinformationen

Für die Interaktion mit Amazon Simple Email Service (Amazon SES) verwenden Sie Sicherheitsanmeldeinformationen, um zu bestätigen, wer Sie sind und ob Sie über die Berechtigung verfügen, mit Amazon SES zu interagieren. Es gibt verschiedene Arten von Anmeldeinformationen. Welche Anmeldeinformationen Sie verwenden, hängt davon ab, was Sie tun möchten. Sie verwenden beispielsweise AWS -Zugriffsschlüssel, wenn Sie eine E-Mail mithilfe der Amazon-SES-API

versenden, und SMTP-Anmeldeinformationen, wenn Sie eine E-Mail über die Amazon-SES-SMTP-Schnittstelle senden.

In der folgenden Tabelle sind die Arten von Anmeldeinformationen aufgeführt, die Sie mit Amazon SES verwenden können, je nachdem, was Sie tun.

Gewünschter Zugriff auf ...	Zu verwenden de Anmeldein formationen	Bestandteile der Anmeldein formationen	Abrufen der Anmeldein formationen
Amazon SES-API (Sie können direkt oder indirekt über ein AWS SDK, das oder das auf die AWS Command Line Interface Amazon SES API zugreifen AWS Tools for Windows PowerShell.)	AWS Zugriffstasten	Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	Informationen finden Sie unter Zugriffsschlüssel in der Allgemeine AWS-Referenz. **Note** Aus Sicherheitsgründen empfiehlt es sich, Benutzerzugriffsschlüssel AWS Identity and Access Management (IAM) anstelle von AWS-Konto Zugriffsschlüsseln zu verwenden. Ihre AWS-Konto Anmeldeinformationen gewähren vollen Zugriff auf all Ihre AWS Ressourcen. Sie sollten sie daher an einem sicheren Ort aufbewahren und stattdessen IAM-Benutzeranmeldedaten für die day-to-day Interaktion mit verwenden.

Gewünschter Zugriff auf ...	Zu verwenden de Anmeldein formationen	Bestandteile der Anmeldein formationen	Abrufen der Anmeldein formationen
			AWS Weitere Informationen finden Sie unter Stammbenutzeranmeldeinformationen vs. IAM-Benutzeranmeldeinformationen in der Allgemeine AWS-Referenz.

Gewünschter Zugriff auf ...	Zu verwenden de Anmeldein formationen	Bestandteile der Anmeldein formationen	Abrufen der Anmeldein formationen
Amazon-SES-SMTP-Schnittstelle	SMTP-Anme ldeinformationen	Benutzername und Passwort	Siehe Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinfo rmationen. **Note** Obwohl sich die Amazon-SES-SMTP-Anmeldeinformationen von Ihren AWS -Zugr iffsschlüsseln und IAM-Benutzerzugrif fsschlüsseln untersche iden, sind Amazon-SE S-SMTP-Anmeldeinfo rmationen tatsächli ch eine Art von IAM-Anmeldeinforma tionen. Ein IAM-Benut zer kann Amazon SES SES-SMTP-Anmeldein formationen erstellen , aber der Inhaber des Root-Kontos muss sicherstellen, dass die Richtlinie des IAM-Benutzers ihm Zugriff auf die folgenden IAM-Aktionen gewährt: „iam: „, „iam: „, ListUsers „iam: „, „iam: CreateUser „und

Gewünschter Zugriff auf ...	Zu verwenden de Anmeldein formationen	Bestandteile der Anmeldein formationen	Abrufen der Anmeldein formationen
			„iam:CreateAccessKey“. PutUserPolicy

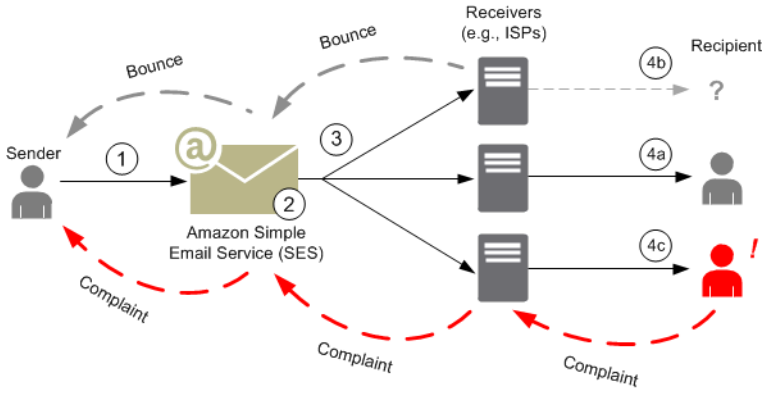
Gewünschter Zugriff auf ...	Zu verwenden de Anmeldein formationen	Bestandteile der Anmeldein formationen	Abrufen der Anmeldein formationen
Amazon SES-Konsole	IAM-Benutzername und -Passwort ODER E-Mail-Adresse und Passwort	IAM-Benutzername und -Passwort ODER E-Mail-Adresse und Passwort	Informationen finden Sie unter IAM-Benutzername und -Passwort und E-Mail-Adresse und Passwort in der Allgemein e AWS-Referenz. **Note** Verwenden Sie als bewährte Sicherhei tsmethode einen IAM-Benutzernamen und ein Passwort anstelle einer E-Mail-Adresse mit einem Passwort. Die Kombination aus E-Mail-Adresse und Passwort ist für Sie bestimmt. Sie sollten sie daher an einem sicheren Ort aufbewahren AWS-Konto, anstatt sie für Interaktionen zu verwenden. day-to-day AWS Weitere Informati onen finden Sie unter Stammbenutzeranmel deinformationen vs. IAM-Benutzeranmeld einformationen in der

Gewünschter Zugriff auf ...	Zu verwenden de Anmeldein formationen	Bestandteile der Anmeldein formationen	Abrufen der Anmeldein formationen
			Allgemeine AWS-Referenz.

Weitere Informationen zu den verschiedenen Typen von AWS Sicherheitsanmeldedaten (mit Ausnahme von SMTP-Anmeldeinformationen, die nur für Amazon SES verwendet werden) finden Sie unter AWS Sicherheitsanmeldedaten in der Allgemeine AWS-Referenz.

Testen der E-Mail-Sendefunktion in Amazon SES

Dieses Thema beschreibt, was geschieht, wenn Sie eine E-Mail mit SES senden, und die verschiedenen Ergebnisse, die auftreten können, nachdem die E-Mail gesendet wurde. Die folgende Abbildung bietet eine allgemeine Übersicht über den Sendevorgang:



1. Eine Client-Anwendung, die als E-Mail-Sender fungiert, stellt eine Anforderung an SES zum Senden von E-Mails an einen oder mehrere Empfänger.
2. Wenn die Anforderung gültig ist, akzeptiert SES die E-Mail.
3. SES sendet die Nachricht über das Internet an den Empfänger. Sobald die Nachricht an SES übergeben ist, wird sie in der Regel sofort gesendet, wobei der erste Zustellungsversuch normalerweise innerhalb von Millisekunden erfolgt.
4. An diesem Punkt gibt es verschiedene Möglichkeiten. Beispiel:

    a. Der ISP stellt die Nachricht dem Posteingang des Empfängers erfolgreich zu.

b. Die E-Mail-Adresse des Empfängers ist nicht vorhanden, sodass der ISP eine Benachrichtigung zur Unzustellbarkeit an SES sendet. SES leitet die Benachrichtigung dann an den Sender weiter.

c. Der Empfänger erhält die Nachricht, stuft sie jedoch als Spam ein und reicht eine Beschwerde beim ISP ein. Der ISP, der eine Feedback-Schleife in SES eingerichtet hat, sendet die Beschwerde an SES, von wo sie an den Sender weitergeleitet wird.

In den folgenden Abschnitten werden die einzelnen Ergebnisse erläutert, die möglich sind, nachdem ein Sender eine E-Mail-Anforderung an SES sendet und nachdem SES eine E-Mail-Nachricht an den Empfänger sendet.

Nachdem ein Sender eine E-Mail-Anforderung an SES sendet

Wenn der Sender eine Anforderung zum Senden einer E-Mail an SES stellt, kann der Aufruf erfolgreich sein oder fehlschlagen. In den folgenden Abschnitten wird beschrieben, was jeweils passiert.

Erfolgreiche Anforderung zum Senden

War die Anforderung an SES erfolgreich, gibt SES eine entsprechende Antwort an den Sender zurück. Diese Nachricht umfasst die Mitteilungs-ID, eine Zeichenfolge, mit der die Anforderung eindeutig identifiziert wird. Sie können die Nachrichten-ID verwenden, um die gesendete E-Mail zu identifizieren oder um Probleme zu verfolgen, die beim Versenden aufgetreten sind (Sie müssen zwischen einer Kennung und der SES-Nachrichten-ID, die SES bei Akzeptanz einer E-Mail an Sie zurückgibt, Ihre eigene Zuordnung speichern). SES stellt dann eine E-Mail-Nachricht basierend auf den Anforderungsparametern zusammen, scannt die Nachricht auf verdächtige Inhalte und Viren und sendet sie über das Internet mit Simple Mail Transfer Protocol (SMTP). Ihre Nachricht wird in der Regel sofort gesendet. Der erste Zustellungsversuch erfolgt normalerweise innerhalb von Millisekunden.

> **Note**
>
> Wenn SES die Anforderung des Absenders akzeptiert und feststellt, dass die Nachricht einen Virus enthält, hält SES die Verarbeitung der Nachricht an und versucht nicht, sie dem E-Mail-Server des Empfängers zuzustellen.

Fehlgeschlagene Anforderung zum Senden

Wenn die Anforderung zum Senden von E-Mails an SES des Senders fehlschlägt, reagiert SES mit einem Fehler und löscht die E-Mail. Die Anforderung kann aus verschiedenen Gründen fehlschlagen. Die Anforderung ist möglicherweise nicht ordnungsgemäß formatiert oder die E-Mail-Adresse wurde vom Sender nicht verifiziert.

Die Methode, mit der Sie ermitteln können, ob die Anforderung fehlgeschlagen ist, hängt davon ab, wie Sie SES aufrufen. Im Folgenden finden Sie einige Beispiele dafür, wie Fehler und Ausnahmen zurückgegeben werden:

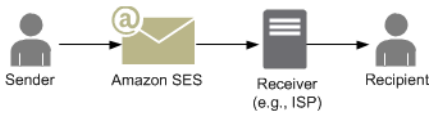
- Wenn Sie SES über die Abfrage (HTTPS) oder API (`SendEmail` oder `SendRawEmail`) aufrufen, geben die Aktionen einen Fehler zurück. Weitere Informationen finden Sie unter der Amazon Simple Notification Service-API-Referenz.
- Wenn Sie ein AWS SDK für eine Programmiersprache verwenden, die Ausnahmen verwendet, löst der Aufruf von SES eine aus MessageRejectedException. (Der Name der Ausnahme kann abhängig vom SDK etwas abweichen.)
- Wenn Sie die SMTP-Schnittstelle verwenden, erhält der Sender einen SMTP-Antwort-Code, doch wie der Fehler weitergeleitet wird, hängt vom Client des Senders ab. Einige Clients zeigen möglicherweise einen Fehlercode an, andere hingegen nicht.

Informationen über die Fehler, die auftreten können, wenn Sie eine E-Mail mit SES senden, finden Sie unter Fehler beim Senden von E-Mails über Amazon SES.

Nachdem Amazon SES eine E-Mail gesendet hat

Wenn die Anforderung des Senders an SES erfolgreich ist, sendet SES die E-Mail mit einem der folgenden Ergebnisse:

- Erfolgreiche Zustellung und der Empfänger lehnt die E-Mail nicht ab – die E-Mail wird vom ISP akzeptiert und der ISP liefert die E-Mail an den Empfänger aus. Eine erfolgreiche Zustellung ist in der folgenden Abbildung dargestellt.

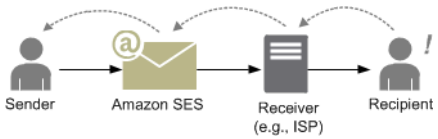


- Permanente Unzustellbarkeit – die E-Mail wird vom ISP aufgrund einer persistenten Bedingung abgelehnt oder sie wird von SES nicht akzeptiert, da die E-Mail-Adresse in der Unterdrückungsliste von SES enthalten ist. Eine E-Mail-Adresse befindet sich auf der SES-Unterdrückungsliste,

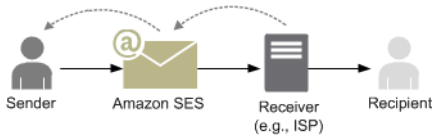
wenn sie kürzlich eine permanente Unzustellbarkeitsnachricht für einen SES-Kunden verursacht hat. Eine permanente Unzustellbarkeit durch einen ISP kann vorliegen, wenn die Adresse des Empfängers ungültig ist. Eine Benachrichtigung über die permanente Unzustellbarkeit wird vom ISP zurück an SES gesendet und von dort wird der Sender entweder per E-Mail oder über Amazon Simple Notification Service (Amazon SNS) benachrichtigt. Die Methode hängt von der Einrichtung des Senders ab. SES benachrichtigt den Sender von Unzustellbarkeiten aufgrund der Unterdrückungsliste mit der gleichen Methode. Der Pfad einer permanenten Unzustellbarkeit für einen ISP ist in der folgenden Abbildung dargestellt.

- Temporäre Unzustellbarkeit – der ISP kann die E-Mail dem Empfänger aufgrund einer temporären Bedingung nicht zustellen. Der ISP ist z. B. zu beschäftigt, um die Anforderung zu bearbeiten, oder das Postfach des Empfängers ist voll. Eine temporäre Unzustellbarkeit kann auch auftreten, wenn die Domäne nicht vorhanden ist. Der ISP sendet eine Benachrichtigung über die temporäre Unzustellbarkeit zurück an SES oder im Falle einer nicht vorhandenen Domäne kann SES keinen E-Mail-Server für die Domäne finden. In beiden Fällen versucht SES über einen längeren Zeitraum, die E-Mail zuzustellen. Wenn SES die E-Mail in diesem Zeitraum nicht ausliefern kann, sendet es Ihnen eine Benachrichtigung über die Unzustellbarkeit per E-Mail oder über Amazon SNS. Wenn SES die E-Mail bei einem der Wiederholungsversuche dem Empfänger zuzustellen kann, ist die Zustellung erfolgreich. Eine temporäre Unzustellbarkeit ist in der folgenden Abbildung dargestellt. In diesem Fall versucht SES wiederholt, die E-Mail zu senden, und der ISP ist schließlich in der Lage, sie dem Empfänger zuzustellen.

- Beschwerde – die E-Mail wird vom ISP akzeptiert und dem Empfänger zugestellt, dieser stuft sie jedoch als Spam ein und klickt auf die Schaltfläche „Als Spam markieren“ in seinem E-Mail-Client. Wenn SES eine Feedback-Schleife für den ISP eingerichtet hat, wird eine Beschwerdebenachrichtigung an SES gesendet, von wo sie an den Sender weitergeleitet wird. Die meisten geben ISPs nicht die E-Mail-Adresse des Empfängers an, der die Beschwerde eingereicht hat. Die Beschwerdebenachrichtigung von SES bietet dem Absender also eine Liste von Empfängern, die die Beschwerde möglicherweise gesendet haben, basierend auf den Empfängern der ursprünglichen Nachricht und dem ISP, von dem SES die Beschwerde erhalten hat. Der Pfad einer Beschwerde ist in der folgenden Abbildung dargestellt.



- Automatische Antwort – die E-Mail wird vom ISP akzeptiert und der ISP stellt sie dem Empfänger zu. Der ISP sendet daraufhin eine automatische Antwort, z. B. eine out-of-the-office (OOTO-) Nachricht, an SES. SES leitet die automatische Antwortbenachrichtigung an den Sender weiter. Eine automatische Antwort ist in der folgenden Abbildung dargestellt.



  Stellen Sie sicher, dass Ihr SES-fähiges Programm nicht erneut versucht, Nachrichten zu senden, die eine automatische Antwort generieren.

> **Tip**
>
> Sie können den SES-Postfachsimulator zum Testen einer erfolgreichen Zustellung, Unzustellbarkeit, Beschwerde, Abwesenheitsnachricht oder der Vorgehensweise, wenn eine Adresse auf der Unterdrückungsliste steht. Weitere Informationen finden Sie unter Manuelles Verwenden des Postfachsimulators.

E-Mail-Format und Amazon SES

Wenn ein Client eine Anforderung an Amazon SES sendet, erstellt Amazon SES eine E-Mail-Nachricht, die mit der Spezifikation für Nachrichtenformate im Internet (RFC 5322) kompatibel ist. Eine E-Mail-Adresse besteht aus einem Header, einem Text und einem Umschlag, wie unten beschrieben.

- Header – Enthält Weiterleitungsanweisungen und Informationen über die Nachricht. Beispiele sind die Senderadresse, die Adresse des Empfängers, der Betreff und das Datum. Der Header ist vergleichbar mit den Informationen im Briefkopf eines Schreibens. Es können jedoch viele andere Arten von Informationen, z. B. das Format der Nachricht, enthalten sein.
- Text – Enthält den eigentlichen Text der Nachricht.
- Umschlag – Enthält die eigentlichen Weiterleitungsinformationen, die zwischen dem E-Mail-Client und dem E-Mail-Server während der SMTP-Sitzung ausgetauscht werden. Diese E-Mail-Umschlaginformationen sind vergleichbar mit den Informationen auf einem postalischen

Umschlag. Die Routing-Informationen des E-Mail-Umschlags sind in der Regel mit den Weiterleitungsinformationen im E-Mail-Header identisch. Es gibt jedoch Ausnahmen. Wenn Sie beispielsweise eine Blindkopie (BCC) senden, entspricht die tatsächliche Empfängeradresse (aus dem Umschlag) nicht der Empfängeradresse, die im E-Mail-Client des Empfängers angezeigt wird, da diese aus dem Header stammt.

Nachfolgend finden Sie ein einfaches Beispiel für eine E-Mail. Auf den Header folgt eine Leerzeile und dann der Text der E-Mail. Der Umschlag wird nicht angezeigt, da er während der SMTP-Sitzung zwischen dem Client und dem E-Mail-Server und nicht als Teil der eigentlichen E-Mail kommuniziert wird.

```
Received: from abc.smtp-out.amazonses.com (123.45.67.89) by in.example.com
 (87.65.43.210); Fri, 17 Dec 2010 14:26:22
From: "Andrew" <andrew@example.com>;
To: "Bob" <bob@example.com>
Date: Fri, 17 Dec 2010 14:26:21 -0800
Subject: Hello
Message-ID: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>
Accept-Language: en-US
Content-Language: en-US
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0

Hello, I hope you are having a good day.

-Andrew
```

In den folgenden Abschnitten überprüfen Sie E-Mail-Header und Texte und ermitteln die Informationen, die Sie angeben müssen, wenn Sie Amazon SES verwenden.

E-Mail-Header

Es ist ein Header pro E-Mail-Nachricht vorhanden. Jede Zeile des Headers enthält ein Feld gefolgt von einem Doppelpunkt und einem Feldtext. Wenn Sie eine E-Mail in einem E-Mail-Client lesen, zeigt dieser Client in der Regel die Werte der folgenden Header-Felder an:

- To – Die E-Mail-Adressen der Empfänger.

- CC – Die E-Mail-Adressen der Empfänger einer Kopie.
- From – Die E-Mail-Adresse, von der die E-Mail gesendet wird.
- Subject – Eine Zusammenfassung des Themas der Nachricht.
- Date – Datum und Uhrzeit, an dem die E-Mail gesendet wird.

Es gibt viele zusätzliche Header-Felder, die Routing-Informationen angeben und den Inhalt der Nachricht beschreiben. E-Mail-Clients zeigen diese Felder dem Benutzer in der Regel nicht an. Eine vollständige Liste der Header-Felder, die Amazon SES akzeptiert, finden Sie unter Amazon SES Header-Felder. Wenn Sie Amazon SES verwenden, müssen Sie den Unterschied zwischen den Header-Feldern "From", "Reply-To" und "Return-Path" verstehen. Wie bereits erwähnt, wird unter "From" die E-Mail-Adresse des Senders der Nachricht angegeben, während "Reply-To" und "Return-Path" wie folgt lauten:

- Reply To – Die E-Mail-Adresse, an die Antworten gesendet werden sollen. Standardmäßig werden die Antworten an die E-Mail-Adresse des ursprünglichen Senders gesendet.
- Return-Path – Die E-Mail-Adresse, an die Unzustellbarkeitsnachrichten und Beschwerden gesendet werden sollen. "Return-Path" wird auch als "envelope from", "envelope sender" oder "MAIL FROM" bezeichnet.

> **Note**
>
> Wenn Sie Amazon SES verwenden, empfehlen wir, dass Sie den Parameter "Return-Path" immer festlegen, sodass Sie über Unzustellbarkeiten informiert werden und entsprechende Korrekturmaßnahmen ergreifen können.

Um eine unzustellbare Nachricht dem geplanten Empfänger einfach zuzuordnen, können Sie Variable Envelope Return Path (VERP) verwenden. Mit VERP legen Sie einen anderen "Return-Path" für jeden Empfänger fest. Wenn die Nachricht nicht zugestellt werden kann, wissen Sie automatisch, für welchen Empfänger sie unzustellbar ist, ohne die Unzustellbarkeitsnachricht öffnen und analysieren zu müssen.

E-Mail-Text

Der E-Mail-Text enthält den eigentlichen Text der Nachricht. Der Text kann in den folgenden Formaten gesendet werden:

- HTML – Wenn der E-Mail-Client des Empfängers HTML interpretieren kann, kann der Text formatierten Text und Hyperlinks enthalten.
- Nur-Text – Wenn der E-Mail-Client des Empfängers textbasiert ist, darf der Text keine nicht druckbaren Zeichen enthalten.
- Sowohl HTML als auch Nur-Text – Wenn Sie beide Formate zum Senden der gleichen Inhalte in einer einzelnen Nachricht verwenden, entscheidet der E-Mail-Client des Empfängers je nach Funktionsumfang, welches Format angezeigt wird.

Wenn Sie eine E-Mail-Nachricht an eine große Anzahl von Empfängern senden, ist es durchaus sinnvoll, sie sowohl als HTML als auch Nur-Text zuzustellen. Einige Empfänger verfügen über HTML-fähige E-Mail-Clients, sodass sie auf eingebettete Hyperlinks in der Nachricht klicken können. Empfänger, die textbasierte E-Mail-Clients verwenden, müssen angeben URLs , dass sie sie mit einem Webbrowser kopieren und öffnen können.

E-Mail-Informationen, die Sie Amazon SES bereitstellen müssen

Wenn Sie eine E-Mail mit Amazon SES senden, hängen die E-Mail-Informationen, die erforderlich sind, davon ab, wie Sie Amazon SES aufrufen. Sie können minimale Informationen angeben und Amazon SES die gesamte Formatierung überlassen. Wenn Sie z. B. eine Anlage senden möchten, können Sie die unformatierte Nachricht selbst bereitstellen. In den folgenden Abschnitten wird erläutert, welche Informationen Sie angeben müssen, wenn Sie eine E-Mail mit der Amazon-SES-API, der Amazon-SES-SMTP-Schnittstelle oder der Amazon-SES-Konsole senden.

Amazon-SES-API

Wenn Sie die Amazon-SES-API direkt aufrufen, rufen Sie entweder die `SendEmail`- oder die `SendRawEmail`-API auf. Die Informationen, die Sie bereitstellen müssen, hängen davon ab, welche API Sie aufrufen.

- Für die `SendEmail API`-API müssen Sie nur eine Quelladresse, eine Empfängeradresse, einen Betreff und den Text angeben. Sie können optional "Antworten an"-Adressen ergänzen. Wenn Sie diese API aufrufen, erstellt Amazon SES automatisch eine ordnungsgemäß formatierte, mehrteilige MIME (Multipurpose Internet Mail Extensions) E-Mail-Nachricht, die für die Darstellung durch E-Mail-Clientsoftware optimiert ist. Weitere Informationen finden Sie unter Senden einer formatierten E-Mail mit der Amazon-SES-API.
- Die API `SendRawEmail` bietet fortgeschrittenen Nutzern die Flexibilität, ihre eigenen Raw-E-Mails mit einem eigenen Header, spezifischen MIME-Teilen und Inhaltsarten zu formatieren und dann zu versenden. `SendRawEmail` wird in der Regel von erfahrenen Benutzern verwendet. Sie müssen

den Nachrichtentext und alle angegebenen Header-Felder bereitstellen, die gemäß Spezifikation für Nachrichtenformate im Internet (RFC 5322) erforderlich sind. Weitere Informationen finden Sie unter Senden von Roh-E-Mails mit der Amazon SES API v2.

Wenn Sie ein AWS SDK verwenden, um die Amazon SES SES-API aufzurufen, geben Sie die oben aufgeführten Informationen an die entsprechenden Funktionen weiter (z. B. `SendEmail` und `SendRawEmail` für Java).

Weitere Informationen zum Senden von E-Mails mit der Amazon-SES-API finden Sie unter Verwenden der Amazon-SES-API zum Senden von E-Mails.

Amazon-SES-SMTP-Schnittstelle

Wenn Sie über die SMTP-Schnittstelle auf Amazon SES zugreifen, erstellt Ihre SMTP-Client-Anwendung die Nachricht, sodass die Informationen, die Sie bereitstellen müssen, von der verwendeten Anwendung abhängen. Für den SMTP-Datenaustausch zwischen einem Client und einem Server sind mindestens eine Quelladresse, eine Zieladresse und Nachrichtendaten erforderlich.

Weitere Informationen zum Senden von E-Mails mit der Amazon-SES-SMTP-Schnittstelle finden Sie unter Verwenden der Amazon-SES-SMTP-Schnittstelle zum Senden von E-Mails.

Amazon-SES-Konsole

Wenn Sie mithilfe der Amazon-SES-Konsole eine E-Mail senden, richtet sich der Umfang der erforderlichen Informationen danach, ob Sie eine formatierte oder Raw-E-Mail senden.

- Für eine formatierte E-Mail müssen Sie eine Quelladresse, eine Zieladresse, einen Betreff und einen Text angeben. Amazon SES erstellt automatisch eine ordnungsgemäß formatierte mehrteilige MIME-E-Mail-Nachricht, die für die Darstellung mit E-Mail-Clientsoftware optimiert ist. Sie können auch eine Feld "Antworten an" und "Antwortpfad bei Unzustellbarkeit" angeben.
- Für eine Raw-E-Mail geben Sie die Quelladresse, eine Zieladresse und den Nachrichteninhalt an, der den Nachrichtentext und alle Header-Felder enthalten muss, die gemäß Spezifikation für Nachrichtenformate im Internet (RFC 5322) erforderlich sind.

Grundlegendes zur E-Mail-Zustellung in Amazon SES

Sie möchten, dass Ihre Empfänger Ihre E-Mails lesen, sie als nützlich erachten und nicht als Spam einstufen. Mit anderen Worten, Sie möchten eine maximale E-Mail-Zustellbarkeit erzielen. Dies

bedeutet, den Prozentanteil der E-Mails zu maximieren, die den Posteingang Ihrer Empfänger erreichen. In diesem Thema werden die wichtigsten Konzepte zur E-Mail-Zustellbarkeit beschrieben. Mit diesen Konzepten sollten Sie vertraut sein, wenn Sie Amazon SES verwenden.

Um eine maximale E-Mail-Zustellbarkeit zu erreichen, müssen Sie wissen, welche grundlegenden Probleme bei der E-Mail-Zustellung auftreten können, und dann proaktive Schritte unternehmen, um diese Probleme zu verhindern. Außerdem benötigen Sie aktuelle Informationen über den Status der von Ihnen gesendeten E-Mails und müssen Ihr E-Mail-Programm bei Bedarf optimieren, um die Wahrscheinlichkeit erfolgreicher Zustellungen zu erhöhen. In den folgenden Abschnitten werden die Konzepte, die diesen Schritten zugrunde liegen, und die Hilfestellung, die Amazon SES während dieses Prozesses leistet, erläutert.

Grundlegende Probleme bei der E-Mail-Zustellung

In den meisten Fällen werden Ihre Nachrichten den Empfängern erfolgreich zugestellt, die sie erwarten. Es kann jedoch vorkommen, dass eine Zustellung fehlschlägt oder ein Empfänger die von Ihnen gesendete E-Mail nicht empfangen möchte. Unzustellbarkeitsnachrichten, Beschwerden und

die Unterdrückungsliste beziehen sich auf diese Probleme bei der Zustellung und werden in den folgenden Abschnitten beschrieben.

Unzustellbarkeit

Wenn der Receiver Ihres Empfängers (z. B. ein ISP) Ihre Nachricht dem Empfänger nicht zustellen kann, sendet er eine Unzustellbarkeitsnachricht an Amazon SES. Amazon SES informiert Sie je nachdem, wie Ihr System eingerichtet ist, per E-Mail oder über Amazon Simple Notification Service (Amazon SNS) über die Unzustellbarkeitsnachricht. Weitere Informationen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.

Dabei wird wie folgt zwischen permanenter Unzustellbarkeit und temporärer Unzustellbarkeit unterschieden:

- Permanente Unzustellbarkeit – Hierbei handelt es sich um einen permanenten E-Mail-Zustellungsfehler. Das Postfach ist beispielsweise nicht vorhanden. Amazon SES versucht bei permanenter Unzustellbarkeit keine erneute Zustellung, mit Ausnahme von DNS-Suchfehlern. Es wird ausdrücklich empfohlen, keine erneuten Zustellversuche an E-Mail-Adressen auszuführen, die eine permanente Unzustellbarkeitsnachricht zurückgeben.
- Temporäre Unzustellbarkeit – Hierbei handelt es sich um einen temporären E-Mail-Zustellungsfehler. Wenn zum Beispiel das Postfach vollständig belegt ist, gibt es zu viele Verbindungen (und es kommt zur Ablehnung) oder die Verbindung läuft ab. Amazon SES führt bei temporärer Unzustellbarkeit mehrere Wiederholungsversuche aus. Wenn die E-Mail dann immer noch nicht zugestellt werden kann, stellt Amazon SES die Zustellversuche ein.

Amazon SES informiert Sie nur über permanente und temporäre Unzustellbarkeiten, bei denen kein erneuter Zustellversuch unternommen wird. Es zählen jedoch nur permanente Unzustellbarkeiten zu Ihrer Unzustellbarkeitsquote und -metrik, die Sie mithilfe der Amazon-SES-Konsole oder `GetSendStatistics`-API abrufen.

Unzustellbarkeiten können entweder synchron oder asynchron sein. Eine synchrone Unzustellbarkeit liegt vor, wenn die E-Mail-Server des Senders und Receivers aktiv kommunizieren. Eine asynchrone Unzustellbarkeit tritt auf, wenn ein Receiver zuerst eine E-Mail für die Zustellung annimmt und diese dann nicht an den Empfänger ausliefern kann.

Beschwerde

Die meisten E-Mail-Client-Programme bieten eine Schaltfläche wie „Als Spam markieren“, über die die Nachricht in einen Spam-Ordner verschoben und an den E-Mail-Anbieter weitergeleitet

wird. Darüber hinaus unterhalten die meisten E-Mail-Anbieter eine Missbrauchsadresse (z. B. abuse@example.net), an die Benutzer unerwünschte E-Mail-Nachrichten weiterleiten und fordern können, dass der E-Mail-Anbieter entsprechende Maßnahmen ergreift, um solche E-Mails zu verhindern. In beiden Fällen reicht der Empfänger eine Beschwerde ein. Wenn der E-Mail-Anbieter zu dem Schluss kommt, dass Sie ein Spammer sind und über Amazon SES eine Feedback-Schleife beim E-Mail-Anbieter eingerichtet wurde, sendet der E-Mail-Anbieter die Beschwerde zurück an Amazon SES. Wenn Amazon SES eine solche Beschwerde erhält, wird sie entweder per E-Mail oder über eine Amazon-SNS-Benachrichtigung an Sie weitergeleitet, je nachdem, wie Ihr System eingerichtet ist. Weitere Informationen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES. Es wird ausdrücklich empfohlen, keine erneuten Zustellversuche an E-Mail-Adressen auszuführen, die zu Beschwerden führen.

Globale Unterdrückungsliste

Die globale Unterdrückungsliste Amazon SES, die sich im Besitz von SES befindet und von SES verwaltet wird, um die Reputation von Adressen im gemeinsam genutzten SES-IP-Pool zu schützen, enthält E-Mail-Adressen von Empfängern, die kürzlich eine permanente Unzustellbarkeit für jeden SES-Kunden verursacht haben. Wenn Sie versuchen, eine E-Mail über SES an eine Adresse zu senden, die auf der Unterdrückungsliste steht, ist der Aufruf an SES erfolgreich, aber SES behandelt die E-Mail als permanente Unzustellbarkeit und sendet sie nicht. Wie alle permanenten Unzustellbarkeiten werden auch Unzustellbarkeiten aufgrund der Unterdrückungsliste bei Ihrer Sendequote und Unzustellbarkeitsquote berücksichtigt. Eine E-Mail-Adresse kann bis zu 14 Tagen auf der Unterdrückungsliste aufgeführt sein. Wenn Sie sicher sind, dass die E-Mail-Adresse, an die Sie senden möchten, gültig ist, können Sie die globale Unterdrückungsliste überschreiben, indem Sie sicherstellen, dass die Adresse nicht in Ihrer Unterdrückungsliste auf Kontoebene aufgeführt ist und SES weiterhin die Zustellung versucht, aber wenn sie zurückgewiesen wird, wirkt sich die Unzustellbarkeit auf Ihre eigene Reputation aus, aber niemand sonst erhält Unzustellbarkeiten, da sie nicht an diese E-Mail-Adresse senden können, wenn sie nicht ihre eigene Unterdrückungsliste auf Kontoebene verwenden. Weitere Informationen zur Unterdrückungsliste der Kontoebene finden Sie unter Verwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole.

Verhalten Sie sich proaktiv

Eines der größten Probleme mit E-Mails im Internet sind unerwünschte Massen-E-Mails (Spam). E-Mail-Anbieter ergreifen umfangreiche Maßnahmen, um zu verhindern, dass ihre Kunden Spam erhalten. Amazon SES ergreift außerdem Schritte, um die Wahrscheinlichkeit zu senken, dass Ihre E-Mails von E-Mail-Anbietern als Spam eingestuft werden. Amazon SES verwendet Verifizierung, Authentifizierung, Sendelimits und Filterung von Inhalten. Amazon SES gilt bei ISPs

als vertrauenswürdig und zuverlässig, sodass Sie angehalten sind, hochgradig erwünschte E-Mails zu senden. Amazon SES übernimmt einige dieser Aufgaben automatisch (z.B. Inhaltsfilterung) bzw. bietet die Tools (z.B. Authentifizierung) oder führt Sie in die richtige Richtung (Sendelimits). In den folgenden Abschnitten erhalten Sie weitere Informationen zu den einzelnen Konzepten.

Verifizierung

Leider können Spammer den Header einer E-Mail fälschen und die ursprüngliche E-Mail-Adresse verschleiern, sodass es so aussieht, als stamme die E-Mail von einer anderen Quelle. Um das Vertrauen zwischen den E-Mail-Anbietern und Amazon SES zu wahren, muss Amazon SES sicherstellen, dass der Sender authentisch ist. Sie müssen daher alle E-Mail-Adressen, von denen Sie E-Mails über Amazon SES senden, zum Schutz Ihrer Identität als Sender verifizieren. Sie können E-Mail-Adressen mit der Amazon-SES-Konsole oder der Amazon-SES-API verifizieren. Sie können auch ganze Domänen verifizieren. Weitere Informationen erhalten Sie unter Erstellen einer E-Mail-Adressidentität und Erstellen einer Domänenidentität.

Ist Ihr Konto noch in der Amazon-SES-Sandbox, müssen Sie außerdem alle Empfängeradressen verifizieren, an die Sie Nachrichten senden, mit Ausnahme derer, die vom Amazon-SES-Postfachsimulator bereitgestellt werden. Weitere Informationen zum Verlassen der Sandbox finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox). Weitere Informationen zum Postfachsimulator finden Sie unter Manuelles Verwenden des Postfachsimulators.

Authentifizierung

DieAuthentifizierung ist eine weitere Möglichkeit, E-Mail-Anbietern zu beweisen, dass Ihre Identität authentisch ist. Bei der Authentifizierung einer E-Mail weisen Sie den ISPs gegenüber nach, dass Sie der Kontoinhaber sind und dass Ihre E-Mails während der Übertragung nicht geändert wurden. Mitunter verweigern Internetdienstanbieter die Weiterleitung von E-Mail, die nicht authentifiziert ist. Amazon SES unterstützt zwei Authentifizierungsmethoden: Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM). Weitere Informationen finden Sie unter Konfigurieren von Identitäten in Amazon SES.

Sendequote

Wenn ein E-Mail-Anbieter plötzliche, unerwartete Spitzen bei der Anzahl oder der Rate Ihrer E-Mails erkennt, könnte er Sie für einen Spammer halten und Ihre E-Mails blockieren. Daher verfügt jedes Amazon-SES-Konto über eine Reihe von Sendekontingenten. Diese Kontingente beschränken die Anzahl der E-Mails, die Sie innerhalb von 24 Stunden senden können, und die Anzahl, die Sie pro Sekunde senden können. Diese Sendekontingente tragen dazu bei, Ihre Vertrauenswürdigkeit bei E-Mail-Anbietern zu schützen.

Wenn Sie ein neuer Benutzer sind, lässt Amazon SES in den meisten Fällen nur eine geringe Anzahl von gesendeten E-Mails pro Tag zu. Wenn die von Ihnen gesendete E-Mail für E-Mail-Anbieter akzeptabel ist, erhöhen wir dieses Kontingent automatisch. Ihre Sendekontingente erhöhen sich im Lauf der Zeit kontinuierlich, sodass Sie E-Mails in größerer Zahl und mit höheren Raten senden können. Darüber hinaus können Sie ein SES Sending Limits Increase-Fall erstellen, um zusätzliche Kontingenterhöhungen anzufordern.

Weitere Informationen zu Sendekontingenten und dazu, wie sie erhöht werden, finden Sie unter Verwalten Ihrer Amazon SES Versandkontingente.

Filterung von Inhalten

Viele E-Mail-Anbieter verwenden die Inhaltsfilterung, um zu bestimmen, ob es sich bei eingehenden E-Mails um Spam handelt. Inhaltsfilter suchen nach fragwürdigen Inhalten und blockieren die E-Mail, wenn sie dem Profil von Spam entsprechen. Amazon SES verwendet ebenfalls Inhaltsfilter. Wenn Ihre Anwendung eine Anforderung an Amazon SES sendet, stellt Amazon SES eine E-Mail-Nachricht in Ihrem Namen zusammen und scannt dann den Header und Text der Nachricht, um festzustellen, ob Inhalte vorliegen, die von E-Mail-Anbietern als Spam betrachtet werden könnten. Wenn Ihre Nachrichten von den Inhaltsfiltern, die Amazon SES verwendet, als Spam eingestuft werden, wirkt sich dies negativ auf Ihre Zuverlässigkeit gegenüber Amazon SES aus.

Amazon SES scannt auch alle Nachrichten auf Viren. Wenn eine Nachricht einen Virus enthält, versucht Amazon SES nicht, dem E-Mail-Server des Empfängers die Nachricht zuzustellen.

Zuverlässigkeit

Im Hinblick auf das Senden von E-Mails ist die Zuverlässigkeit wichtig. Sie ist ein Maß für das Vertrauen darauf, dass eine IP-Adresse, E-Mail-Adresse oder sendende Domäne keinen Spam verursacht. Amazon SES gilt bei ISPs als sehr zuverlässig, sodass Ihre E-Mails den Posteingang Ihrer Empfänger erreichen. Entsprechend müssen Sie vertrauenswürdige Zuverlässigkeit gegenüber Amazon SES beweisen. Sie bauen Ihren Zuverlässigkeit bei Amazon SES auf, indem Sie hochwertige Inhalte senden. Wenn Sie hochwertige Inhalte senden, wird Ihre Zuverlässigkeit mit der Zeit vertrauenswürdiger und Amazon SES erhöht Ihre Sendequoten. Übermäßige Unzustellbarkeiten und Beschwerden wirken sich negativ auf Ihre Zuverlässigkeit aus und können dazu veranlassen, die Sendekontingente für Ihr Konto zu reduzieren oder Ihr Amazon-SES-Konto zu beenden.

Eine Möglichkeit, Ihre Zuverlässigkeit zu wahren, ist die Verwendung des Postfachsimulators, wenn Sie Ihr System testen, anstatt Nachrichten an E-Mail-Adressen zu senden, die Sie selbst erstellt haben. E-Mails an den Postfachsimulator werden bei den Metriken zu Unzustellbarkeitsnachrichten

und Beschwerden nicht berücksichtigt. Weitere Informationen zum Postfachsimulator finden Sie unter Manuelles Verwenden des Postfachsimulators.

Hochgradig erwünschte E-Mail

Hochgradig erwünschte E-Mail sind E-Mails, die Empfänger als wertvoll erachten und die sie erhalten möchten. „Wertvoll“ wird von unterschiedlichen Empfängern auch unterschiedlich definiert und kann z. B. Angebote, Auftragsbestätigen, Belege und Newsletter umfassen. Die Zustellbarkeit hängt letztendlich von der Qualität der E-Mails ab, die Sie senden, da E-Mail-Anbieter E-Mails blockieren, die sie als geringwertig betrachten.

Bleiben Sie auf dem Laufenden

Ganz gleich, ob Ihre Zustellungen fehlschlagen, Ihre Empfänger sich über Ihre E-Mails beschweren oder Amazon SES eine E-Mail an den Mailserver eines Empfängers übermittelt, hilft Ihnen dabei, das Problem zu ergründen, indem Benachrichtigungen und die Möglichkeit der Überwachung Ihrer Nutzungsstatistiken bereitgestellt werden.

Benachrichtigungen

Wenn eine E-Mail zu einer Unzustellbarkeitsnachricht führt, benachrichtigt der E-Mail-Anbieter Amazon SES und Amazon SES informiert Sie darüber. Amazon SES informiert Sie nur über permanente und temporäre Unzustellbarkeiten, bei denen kein erneuter Zustellversuch unternommen wird. Viele ISPs leiten Beschwerden außerdem weiter und Amazon SES richtet Feedback-Schleifen für Beschwerden für alle großen ISPs ein, sodass Sie diesen Schritt nicht selbst ausführen müssen. Amazon SES kann Sie über Unzustellbarkeiten, Beschwerden und erfolgreiche Zustellungen auf zwei Arten benachrichtigen: Sie können Ihr Konto für den Empfang von Benachrichtigungen über Amazon SNS einrichten oder Benachrichtigungen per E-Mail empfangen (nur Unzustellbarkeiten und Beschwerden). Weitere Informationen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.

Nutzungsstatistiken

Amazon SES bietet Nutzungsstatistiken, sodass Sie fehlgeschlagene Zustellungen ansehen können, um die Ursachen zu identifizieren und zu beheben. Sie können Ihre Nutzungsstatistiken mithilfe der Amazon-SES-Konsole oder durch Aufrufen der Amazon-SES-API einsehen. Sie können die Anzahl von Zustellungen, Unzustellbarkeitsnachrichten, Beschwerden und virenverseuchten E-Mails ansehen und sich Ihre Sendekontingente anzeigen lassen, um sicherzustellen, dass Sie Ihre Kontingente einhalten.

Verbessern Sie Ihr E-Mail-Programm

Wenn Sie eine große Zahl von Unzustellbarkeitsnachrichten und Beschwerden erhalten, sollten Sie Ihre Strategie für das Senden von E-Mail optimieren. Denken Sie daran, dass übermäßige Zurückweisungen, Beschwerden und Versuche, E-Mails von schlechter Qualität zu versenden, Missbrauch darstellen und Sie dem AWS-Konto Risiko einer Kündigung aussetzen. Letztendlich müssen Sie sicher sein, dass Sie Amazon SES verwenden, um hochgradig erwünschte E-Mails zu senden und zwar nur an Empfänger, die diese E-Mails erhalten möchten.

At-least-once Lieferung

Amazon SES speichert aus Gründen der Redundanz und Hochverfügbarkeit Kopien der Nachrichten auf mehreren Servern. In seltenen Fällen kann es vorkommen, dass einer der Server, auf dem eine Nachrichtenkopie gespeichert ist, nicht verfügbar ist, wenn Sie eine Nachricht erhalten oder löschen.

In diesem Fall wird die Kopie der Nachricht auf dem nicht verfügbaren Server nicht gelöscht und Sie erhalten diese Nachrichtenkopie erneut, wenn Sie Nachrichten empfangen. Konzipieren Sie Ihre Anwendungen idempotent (d. h., die mehrmalige Verarbeitung derselben Nachricht darf die Anwendung nicht nachteilig beeinflussen).

Bewährte Methoden für das Versenden von E-Mails mit Amazon SES

Die Art und Weise, wie Sie die E-Mail-Kommunikation mit Ihren Kunden verwalten, wird als Ihr E-Mail-Programm bezeichnet. Es gibt mehrere Faktoren, die zum Erfolg oder Misserfolg Ihres E-Mail-Programms führen können. Diese Faktoren können zunächst verwirrend oder mysteriös erscheinen. Indem Sie verstehen, wie E-Mails zugestellt werden, und indem Sie bestimmte bewährte Methoden befolgen, können Sie die Chancen erhöhen, dass Ihre E-Mails erfolgreich die Posteingänge Ihrer Kunden erreichen.

Themen

- Erfolgsmetriken von E-Mail-Programmen
- Aufrechterhaltung einer positiven Reputation als Absender

Erfolgsmetriken von E-Mail-Programmen

Es gibt mehrere Metriken, die den Erfolg Ihres E-Mail-Programms messen können.

Dieser Abschnitt enthält Informationen zu den folgenden Metriken:

- Unzustellbarkeit

- Complaints (Beschwerden)
- Nachrichtenqualität

Unzustellbarkeit

Eine Unzustellbarkeit tritt auf, wenn eine E-Mail nicht an den vorgesehenen Empfänger zugestellt werden kann. Es gibt zwei Arten von Unzustellbarkeiten: permanente Unzustellbarkeit und temporäre Unzustellbarkeit. Eine permanente Unzustellbarkeit tritt auf, wenn die E-Mail aufgrund eines anhaltenden Problems nicht zugestellt werden kann, z. B. wenn eine E-Mail-Adresse nicht vorhanden ist. Eine temporäre Unzustellbarkeit liegt vor, wenn ein temporäres Problem die Zustellung einer E-Mail verhindert. Temporäre Unzustellbarkeiten können auftreten, wenn der Posteingang eines Empfängers voll ist oder wenn der empfangende Server vorübergehend nicht verfügbar ist. Amazon SES versucht bei temporärer Unzustellbarkeit, die entsprechenden E-Mails für einen bestimmten Zeitraum erneut zuzustellen.

Es ist unerlässlich, dass Sie die Anzahl der permanenten unzustellbaren E-Mails in Ihrem E-Mail-Programm überwachen und permanente unzustellbare E-Mail-Adressen aus Ihren Empfängerlisten entfernen. Wenn E-Mail-Empfänger eine hohe Rate an permanente Unzustellbarkeiten feststellen, gehen sie davon aus, dass Sie Ihre Empfänger nicht gut kennen. Daher kann eine hohe permanente Unzustellbarkeitsrate die Zustellbarkeit Ihrer E-Mail-Nachrichten negativ beeinflussen.

Die folgenden Richtlinien helfen Ihnen, unzustellbare E-Mails zu vermeiden und Ihre Zuverlässigkeit als Absender zu verbessern:

- Versuchen Sie, Ihre permanent unzustellbaren E-Mails unter 5% zu halten. Je weniger Hardbounces Ihr E-Mail-Programm enthält, desto wahrscheinlicher ist es, dass Ihre Nachrichten als legitim und wertvoll angesehen ISPs werden. Diese Rate sollte als vernünftiges und erreichbares Ziel angesehen werden, ist aber keine allgemeingültige Regel. ISPs
- Mieten oder kaufen Sie niemals E-Mail-Listen. Diese Listen können eine große Anzahl ungültiger Adressen enthalten, was dazu führen kann, dass sich Ihre permanent unzustellbaren E-Mails drastisch erhöhen. Darüber hinaus können diese Listen Spam-Traps enthalten – E-Mail-Adressen, die speziell dazu verwendet werden, um illegale Absender zu ermitteln. Wenn Ihre Nachrichten in einer Spam-Trap landen, können Ihre Zustellraten und die Zuverlässigkeit des Senders unwiderruflich beschädigt werden.
- Halten Sie Ihre Liste auf dem neuesten Stand. Wenn Sie Ihre Empfänger seit langem nicht mehr per E-Mail benachrichtigt haben, versuchen Sie, den Status Ihrer Kunden auf andere Weise zu überprüfen (z. B. durch Anmeldeaktivitäten auf der Website oder die Kaufhistorie).

- Wenn Sie keine Möglichkeit haben, den Status Ihrer Kunden zu verifizieren, sollten Sie sich überlegen, ob Sie eine Rückgewinnungs-E-Mail versenden möchten. Eine typische Rückgewinnungs-E-Mail erwähnt, dass Sie seit einiger Zeit nichts mehr von dem Kunden gehört haben, und ermutigt den Kunden zu bestätigen, dass er Ihre E-Mail weiterhin erhalten möchte. Nach dem Versenden einer Rückgewinnungs-E-Mail löschen Sie alle Empfänger, die nicht geantwortet haben, aus Ihren Listen.

Wenn Sie unzustellbare E-Mails erhalten, ist es wichtig, dass Sie auf diese angemessen reagieren, indem Sie die folgenden Regeln beachten:

- Wenn eine E-Mail-Adresse permanent unzustellbar ist, entfernen Sie die Adresse sofort aus Ihren Listen. Versuchen Sie nicht, erneut Nachrichten an unzustellbare Adressen zu senden. Wiederholte unzustellbare E-Mails summieren sich und schaden letztendlich Ihrer Zuverlässigkeit beim ISP des Empfängers.
- Stellen Sie sicher, dass die Adresse, die Sie verwenden, um Benachrichtigungen über die Unzustellbarkeit zu erhalten, E-Mails empfangen kann. Weitere Informationen zum Einrichten von Unzustellbarkeits- und Beschwerdebenachrichtigungen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.
- Wenn Ihre eingehende E-Mail von einem ISP zu Ihnen gelangt, anstatt über Ihre eigenen internen Server, kann eine hohe Menge von Benachrichtigungen über die Unzustellbarkeit in Ihrem Spam-Ordner landen oder ganz entfallen. Idealerweise sollten Sie keine gehostete E-Mail-Adresse verwenden, um unzustellbare E-Mails zu erhalten. Wenn dies zwingend erforderlich ist, prüfen Sie den Spam-Ordner regelmäßig und markieren Sie die Unzustellbarkeits-E-Mails nicht als Spam. In Amazon SES können Sie die Adresse angeben, an die Benachrichtigungen über die Unzustellbarkeit gesendet werden.
- Normalerweise liefert eine Unzustellbarkeitsbenachrichtigung die Adresse des Postfachs, das die Zustellung verweigert. Wenn Sie jedoch detailliertere Daten benötigen, um eine Empfängeradresse einer bestimmten E-Mail-Kampagne zuzuordnen, fügen Sie einen X-Header mit einem Wert hinzu, den Sie über Ihr internes Tracking-System zurückverfolgen können. Weitere Informationen finden Sie unter Amazon SES Header-Felder.

Complaints (Beschwerden)

Eine Beschwerde liegt vor, wenn ein E-Mail-Empfänger in seinem webbasierten E-Mail-Client auf die Schaltfläche „Als Spam markieren“ (oder gleichwertig) klickt. Wenn Sie eine große Anzahl dieser Beschwerden anhäufen, geht der ISP davon aus, dass Sie Spam versenden. Dies wirkt sich

negativ auf die Zustellbarkeitsrate und die Reputation des Absenders aus. Einige, aber nicht alle, benachrichtigen Sie, wenn eine Beschwerde gemeldet ISPs wird. Dies wird als Feedback-Schleife bezeichnet. Amazon SES leitet Beschwerden aus ISPs diesen Feedback-Schleifen automatisch an Sie weiter.

Die folgenden Richtlinien helfen Ihnen, Beschwerden zu vermeiden und Ihre Zuverlässigkeit als Absender zu verbessern:

- Versuchen Sie, Ihre Beschwerdequote unter 0,1% zu halten. Je weniger Beschwerden in Ihrem E-Mail-Programm enthalten sind, desto wahrscheinlicher ist es, dass Ihre Nachrichten als legitim und wertvoll angesehen ISPs werden. Diese Quote sollte als vernünftiges und erreichbares Ziel angesehen werden, ist aber keine allgemeingültige Regel. ISPs
- Wenn sich ein Kunde über eine Marketing-E-Mail beschwert, sollten Sie sofort damit aufhören, diesem Kunden Marketing-E-Mails zu senden. Wenn Ihr E-Mail-Programm jedoch auch andere Arten von E-Mails umfasst (z. B. Benachrichtigungen oder Transaktions-E-Mails), kann es akzeptabel sein, diese Arten von Nachrichten weiterhin an den Empfänger mit der Beschwerde zu senden.
- Wenn Sie eine Liste haben, an die Sie seit einiger Zeit keine E-Mails mehr gesendet haben, stellen Sie sicher, dass Ihre Empfänger verstehen, warum sie Ihre Nachrichten erhalten. Wir empfehlen Ihnen, eine Willkommensnachricht zu senden, die Sie daran erinnert, wer Sie sind und warum Sie sie kontaktieren.

Wenn Sie Beschwerden erhalten, ist es unerlässlich, dass Sie auf diese angemessen reagieren, indem Sie die folgenden Regeln beachten:

- Stellen Sie sicher, dass die Adresse, die Sie verwenden, um Beschwerdebenachrichtigungen zu erhalten, E-Mails empfangen kann. Weitere Informationen zum Einrichten von Unzustellbarkeits- und Beschwerdebenachrichtigungen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.
- Stellen Sie sicher, dass Ihre Beschwerdebenachrichtigungen nicht von Ihrem ISP oder Mailsystem als Spam markiert werden.
- Beschwerdebenachrichtigungen enthalten in der Regel den Text der E-Mail. Dies unterscheidet sich von Benachrichtigungen über die Unzustellbarkeit, die typischerweise nur die E-Mail-Header enthalten. In Beschwerdebenachrichtigungen wird jedoch in der Regel die E-Mail-Adresse der Person, die sich beschwert hat, entfernt. Verwenden Sie benutzerdefinierte X-Header oder spezielle Identifikatoren, die in den E-Mail-Text eingebettet sind, damit Sie die E-Mail-Adresse

identifizieren können, die die Beschwerde gesendet hat. Auf diese Weise können Sie Adressen, von denen Beschwerden stammen, leichter identifizieren, sodass Sie sie aus Ihren Empfängerlisten entfernen können.

Nachrichtenqualität

E-Mail-Empfänger verwenden Inhaltsfilter, um bestimmte Attribute in Ihren Nachrichten zu erkennen. So können sie feststellen, ob Ihre Nachricht legitim ist. Diese Inhaltsfilter überprüfen automatisch den Inhalt Ihrer Nachrichten, um gemeinsame Merkmale von unerwünschten und bösartigen Nachrichten zu identifizieren. Amazon SES verwendet Inhaltsfiltertechnologien, um Nachrichten mit Malware vor dem Versenden zu erkennen und zu blockieren.

Wenn die Inhaltsfilter eines E-Mail-Empfängers feststellen, dass Ihre Nachricht die Merkmale von Spam oder bösartigen E-Mails enthält, wird Ihre Nachricht höchstwahrscheinlich markiert und aus den Posteingangsfächern der Empfänger entfernt.

Bedenken Sie die folgenden Punkte, wenn Sie Ihre E-Mail gestalten:

- Moderne Inhaltsfilter sind intelligent, passen sich kontinuierlich an und verändern sich. Sie verlassen sich nicht auf ein vordefiniertes Regelwerk. Dienste von Drittanbietern wie ReturnPathLitmus können dir dabei helfen, Inhalte in deiner E-Mail zu identifizieren, die Inhaltsfilter auslösen könnten.
- Wenn deine E-Mail Links enthält, überprüfe anhand von DNS-basierten Blackhole-Listen (DNSBLs), wie sie auf Uribl.com und Surbl.org zu finden sind, ob diese Links vorhanden sind. URLs
- Vermeiden Sie die Verwendung von Linkverkürzern. Böswillige Absender können Linkverkürzungen verwenden, um das tatsächliche Ziel eines Links zu verbergen. Wenn ISPs Sie feststellen, dass Dienste zum Verkürzen von Links — selbst die seriösesten — für schändliche Zwecke genutzt werden, können sie den Zugriff auf diese Dienste ganz verweigern. Enthält Ihre E-Mail einen Link zu einem Link auf einer schwarzen Liste, erreicht sie nicht die Posteingänge Ihrer Kunden und der Erfolg Ihrer E-Mail-Kampagne leidet darunter.
- Testen Sie jeden Link in Ihrer E-Mail, um sicherzustellen, dass er auf die gewünschte Seite verweist.
- Stellen Sie sicher, dass Ihre Website Datenschutzrichtlinien und Nutzungsbedingungen enthält und dass diese Dokumente auf dem neuesten Stand sind. Es ist ein bewährtes Verfahren, in jeder gesendeten E-Mail auf diese Dokumente zu verlinken. Die Bereitstellung von Links zu

diesen Dokumenten zeigt, dass Sie nichts vor Ihren Kunden zu verbergen haben. Dies kann ein Vertrauensverhältnis fördern.

- Wenn Sie hochfrequente Inhalte (z. B. „Tagesangebot“) versenden möchten, achten Sie darauf, dass der Inhalt Ihrer E-Mails bei jedem Einsatz unterschiedlich ist. Wenn Sie Nachrichten mit hoher Frequenz versenden, müssen Sie sicherstellen, dass diese Nachrichten zeitgerecht und relevant sind. Sie sollten sich nicht wiederholen oder störend sein.

Aufrechterhaltung einer positiven Reputation als Absender

In Amazon SES bezieht sich die Absenderreputation auf die Glaubwürdigkeit und Vertrauenswürdigkeit des E-Mail-Absenders, wie sie von E-Mail-Anbietern und Spam-Filtern wahrgenommen wird. Es ist ein Maß dafür, wie wahrscheinlich es ist, dass Ihre E-Mails als legitim eingestuft und erfolgreich an die Posteingänge der Empfänger zugestellt werden.

In den folgenden Abschnitten werden die wichtigsten Prinzipien des E-Mail-Versands vorgestellt, auf die Sie achten müssen, um sicherzustellen, dass Ihre E-Mail-Kommunikation Ihre Zielgruppe erreicht und gleichzeitig einen guten Ruf als Absender bewahrt.

Überlegungen zur Domäne und zur „From“-Adresse

- Denken Sie sorgfältig über die Adressen nach, von denen Sie E-Mails versenden. Die „From“-Adresse ist eine der ersten Informationen, die Ihre Empfänger sehen. Sie kann somit einen bleibenden ersten Eindruck hinterlassen. Darüber hinaus ISPs verknüpfen einige Ihren Ruf mit Ihrer Absenderadresse.
- Ziehen Sie in Betracht, Unterdomänen für verschiedene Kommunikationsarten zu verwenden. Nehmen wir zum Beispiel an, dass Sie E-Mails von der Domäne example.com senden und planen, sowohl Marketing- als auch Transaktionsnachrichten zu versenden. Anstatt alle Ihre Nachrichten von example.com zu versenden, senden Sie Ihre Marketing-Nachrichten von einer Unterdomäne wie marketing.example.com und Ihre transaktionalen Nachrichten von einer Unterdomäne wie orders.example.com. Eindeutige Unterdomänen entwickeln ihre eigene Reputation. Der Einsatz von Unterdomänen reduziert das Risiko von Reputationsschäden, wenn z. B. Ihre Marketingkommunikation in einer Spam-Trap landet oder einen Inhaltsfilter auslöst.
- Wenn Sie planen, eine große Anzahl von Nachrichten zu versenden, sollten Sie diese Nachrichten nicht von einer ISP-basierten Adresse wie sender@hotmail.com aus versenden. Wenn ein ISP eine große Menge an Nachrichten von sender@hotmail.com bemerkt, wird diese E-Mail anders behandelt als eine E-Mail, die von einer Domäne in Ihrem Besitz stammt.

- Arbeiten Sie mit Ihrer Domänenvergabestelle zusammen, um sicherzustellen, dass die WHOIS-Informationen für Ihre Domäne korrekt sind. Wenn Sie einen ehrlichen und up-to-date WHOIS-Eintrag führen, zeigen Sie, dass Sie Wert auf Transparenz legen, und ermöglicht es Benutzern, schnell zu erkennen, ob Ihre Domain legitim ist oder nicht.
- Vermeiden Sie es, eine no-reply-Adresse, wie z. B. no-reply@example.com als „From“- oder „Reply-to“-Adresse zu verwenden. Die Verwendung einer no-reply@-E-Mail-Adresse sendet Ihren Empfängern eine klare Botschaft: Sie bieten ihnen keine Möglichkeit, mit Ihnen in Kontakt zu treten. Sie sind nicht an Feedback interessiert.

Authentifizierung

- Authentifizieren Sie Ihre Domäne mit SPF und SenderID. Diese Authentifizierungsmethoden bestätigen den E-Mail-Empfängern, dass jede von Ihnen gesendete E-Mail tatsächlich von der angegebenen Domäne stammt.
- Signieren Sie Ihre ausgehenden E-Mails mit DKIM. Dieser Schritt bestätigt den Empfängern, dass der Inhalt während der Übertragung zwischen Sender und Empfänger nicht verändert wurde.
- Sie können Ihre Authentifizierungseinstellungen für SPF und DKIM testen, indem Sie eine E-Mail an eine eigene, ISP-basierte E-Mail-Adresse senden (z. B. ein persönliches Google Mail- oder Hotmail-Konto) und dann die Header der Nachricht anzeigen. Die Header zeigen an, ob Ihre Versuche, die Nachricht zu authentifizieren und zu signieren, erfolgreich waren.

Erstellen und Pflegen von Listen

- Umsetzung einer Double-Opt-In-Strategie. Wenn sich Benutzer anmelden, um E-Mails von Ihnen zu erhalten, senden Sie ihnen eine Nachricht mit einem Bestätigungslink. Fangen Sie nicht an, ihnen E-Mails zu senden, bis sie ihre Adresse mit einem Klick auf den Link bestätigen. Eine Double-Opt-In-Strategie senkt die Menge der durch Tippfehler verursachten Menge an permanent unzustellbaren E-Mails.
- Wenn Sie E-Mail-Adressen mit einem webbasierten Formular erfassen, führen Sie eine minimale Prüfung dieser Adressen bei der Übermittlung durch. Stellen Sie z. B. sicher, dass die gesammelten Adressen wohlgeformt sind (d. h. im Format recipient@example.com) und dass sie sich auf Domänen mit gültigen MX-Einträgen beziehen.
- Seien Sie vorsichtig, wenn benutzerdefinierte Eingaben ungeprüft an Amazon SES übergeben werden. Forenregistrierungen und gesendete Formulare stellen ein einzigartiges Risiko dar. Der Inhalt ist vollständig benutzergeneriert und Spammer können Formulare mit eigenem Inhalt

ausfüllen. Sie müssen sicherstellen, dass Sie nur E-Mails mit qualitativ hochwertigen Inhalten versenden.

- Es ist sehr unwahrscheinlich, dass sich ein Standard-Alias (wie postmaster@, abuse@ oder noc@) jemals absichtlich für Ihre E-Mail registriert. Stellen Sie sicher, dass Sie nur Nachrichten an echte Personen senden, die diese auch wirklich empfangen möchten. Diese Regel gilt insbesondere für Standard-Aliase, die üblicherweise für E-Mail-Watchdogs reserviert sind. Diese Aliase können gezielt als Sabotage in Ihre Liste aufgenommen werden, um Ihre Reputation zu schädigen.

Compliance

- Beachten Sie die Gesetze und Vorschriften für das E-Mail-Marketing und Anti-Spam für die Länder und Regionen, an die Sie E-Mails senden. Sie sind dafür verantwortlich, sicherzustellen, dass die von Ihnen gesendeten E-Mails diese Gesetze erfüllen. Dieses Handbuch deckt diese Gesetze nicht ab, daher ist es wichtig, dass Sie sich darüber informieren. Eine Liste der Gesetze finden Sie unter Email Spam Legislation by Country auf Wikipedia.
- Wenden Sie sich immer an einen Rechtsanwalt, um juristischen Rat einzuholen.

Amazon SES mit einem AWS SDK verwenden

AWS Software Development Kits (SDKs) sind für viele beliebte Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK für C++	AWS SDK für C++ Codebeispiele
AWS CLI	AWS CLI Code-Beispiele
AWS SDK für Go	AWS SDK für Go Code-Beispiele
AWS SDK für Java	AWS SDK für Java Code-Beispiele
AWS SDK für JavaScript	AWS SDK für JavaScript Code-Beispiele
AWS SDK für Kotlin	AWS SDK für Kotlin Code-Beispiele

SDK-Dokumentation	Codebeispiele
AWS SDK für .NET	AWS SDK für .NET Code-Beispiele
AWS SDK für PHP	AWS SDK für PHP Code-Beispiele
AWS -Tools für PowerShell	AWS -Tools für PowerShell Code-Beispiele
AWS SDK für Python (Boto3)	AWS SDK für Python (Boto3) Code-Beispiele
AWS SDK für Ruby	AWS SDK für Ruby Code-Beispiele
AWS SDK für Rust	AWS SDK für Rust Code-Beispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Code-Beispiele
AWS SDK für Swift	AWS SDK für Swift Code-Beispiele

Weitere Beispiele für Amazon SES finden Sie unter Codebeispiele für Amazon SES mit AWS SDKs.

> **Beispiel für die Verfügbarkeit**
>
> Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Provide feedback (Feedback geben) auswählen.

Erste Schritte mit Amazon Simple Storage Service

Dieses Kapitel führt Sie durch die Aufgaben, die für die erstmalige Einrichtung von Amazon SES erforderlich sind, sowie Tutorials, die Ihnen den Einstieg erleichtern.

Topics

- Amazon Simple Email Service einrichten
- Migration zu Amazon SES von einer anderen E-Mail-Sendelösung
- Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox)

Amazon Simple Email Service einrichten

Bevor Sie Amazon SES verwenden können, müssen Sie die folgenden Schritte ausführen.

Aufgaben

- Melde dich an für AWS
- Einrichten Ihres SES-Kontos
- Gewähren Sie programmatischen Zugriff (um außerhalb der Konsole mit SES zu interagieren)
- Laden Sie ein AWS SDK herunter (zur Verwendung des SES APIs)

Melde dich an für AWS

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Einrichten Ihres SES-Kontos

Beginnen Sie mit SES, indem Sie eine E-Mail-Adresse verifizieren und eine Domain senden, sodass Sie mit dem Senden von E-Mails über SES beginnen und mithilfe des SES-Kontoeinrichtungsassistenten Produktionszugriff für Ihr Konto beantragen können.

Verwenden Ihres SES-Kontoeinrichtungsassistenten zum Einrichten Ihres Kontos

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie auf der Startseite der SES-Konsole die Option Erste Schritte aus. Der Assistent führt Sie dann durch die einzelnen Schritte zur Einrichtung Ihres SES-Kontos.

Der Assistent zur Einrichtung eines SES-Kontos wird nur angezeigt, wenn Sie noch keine Identitäten (E-Mail-Adresse oder Domain) in SES erstellt haben.

Gewähren Sie programmatischen Zugriff (um außerhalb der Konsole mit SES zu interagieren)

Benutzer benötigen programmgesteuerten Zugriff, wenn sie mit AWS außerhalb des AWS-Managementkonsole interagieren möchten. Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Empfohlen) Verwenden Sie Konsolenanmeldeinformationen als temporäre Anmeldeinformationen, um programmatische Anfragen an AWS CLI AWS SDKs, oder zu signieren . AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zum AWS CLI finden Sie unter Anmeldung für AWS lokale Entwicklung im AWS Command

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		Line Interface Benutzerh andbuch. • Weitere Informationen finden Sie unter Anmeldung für AWS lokale Entwicklu ng im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. AWS SDKs
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.	Befolgen Sie die Anweisung en für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch AWS SDKs und im Tools-Ref erenzhandbuch.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu AWS CLI finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldeinformationen im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. • Weitere Informationen finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. AWS APIs

Laden Sie ein AWS SDK herunter (zur Verwendung des SES APIs)

Um den SES aufzurufen, APIs ohne sich um Details auf niedriger Ebene wie das Zusammenstellen von HTTP-Anfragen kümmern zu müssen, können Sie ein AWS SDK verwenden. AWS SDKs Sie stellen Funktionen und Datentypen bereit, die die Funktionalität von SES und anderen Diensten zusammenfassen. AWS Um ein AWS SDK herunterzuladen, gehen Sie zu. SDKs Nachdem Sie das SDK heruntergeladen haben, erstellen Sie eine Datei mit gemeinsamen Anmeldeinformationen und geben Sie Ihre AWS Zugriffsschlüssel an.

Migration zu Amazon SES von einer anderen E-Mail-Sendelösung

Dieses Thema bietet einen Überblick über die Schritte, die Sie ausführen müssen, wenn Sie Ihre E-Mail-Sendelösung von einer On-Premises gehosteten Lösung oder von einer auf einer Amazon-EC2-Instance gehosteten Lösung auf Amazon SES verschieben möchten.

Themen in diesem Abschnitt:

- Schritt 1. Überprüfen Ihrer Domäne
- Schritt 2. Anfordern von Produktionszugriff.
- Schritt 3. Konfigurieren von Domänenauthentifizierungssystemen
- Schritt 4. Erstellen Ihrer SMTP-Anmeldeinformationen
- Schritt 5. Herstellen einer Verbindung mit einem SMTP-Endpunkt
- Nächste Schritte

Schritt 1. Überprüfen Ihrer Domäne

Bevor Sie E-Mail-Nachrichten mit Amazon SES versenden können, müssen Sie die Identitäten überprüfen, von denen Sie E-Mail-Nachrichten senden möchten. In Amazon SES kann eine Identität eine E-Mail-Adresse oder eine ganze Domäne sein. Wenn Sie eine Domäne überprüfen, können Sie mit Amazon SES E-Mails von einer beliebigen Adresse in dieser Domäne aus senden. Weitere Informationen zum Verifizieren von Domänen finden Sie unter Erstellen einer Domänenidentität.

Schritt 2. Anfordern von Produktionszugriff.

Wenn Sie Amazon SES das erste Mal verwenden, befindet sich Ihr Konto in einer Sandbox-Umgebung. Während sich Ihr Konto in der Sandbox befindet, können Sie nur E-Mail-Nachrichten an Adressen und Domänen senden, die Sie verifiziert haben. Darüber hinaus gibt es Einschränkungen für die Anzahl der Nachrichten, die Sie pro Tag senden können, und die Anzahl, die Sie pro Sekunde senden können. Weitere Hinweise zum Anfordern des Produktionszugriffs finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).

Schritt 3. Konfigurieren von Domänenauthentifizierungssystemen

Sie können Ihre Domäne so konfigurieren, dass Authentifizierungssysteme wie DKIM und SPF verwendet werden. Dieser Schritt ist technisch gesehen optional. Durch die Einrichtung von DKIM oder SPF (oder beider) für Ihre Domäne können Sie die Zustellbarkeit Ihrer E-Mail-Nachrichten

verbessern und das Vertrauen Ihrer Kunden erhöhen. Weitere Informationen zur Einrichtung von SPF finden Sie unter Authentifizierung Ihrer E-Mails mit SPF in Amazon SES. Weitere Informationen zur Einrichtung von DKIM finden Sie unter Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES.

Schritt 4. Erstellen Ihrer SMTP-Anmeldeinformationen

Wenn Sie planen, E-Mail-Nachrichten mit einer Anwendung zu senden, die SMTP verwendet, müssen Sie SMTP-Anmeldeinformationen generieren. Ihre SMTP-Anmeldeinformationen sind nicht mit den regulären AWS -Anmeldeinformationen identisch. Diese Anmeldeinformationen sind außerdem in jeder AWS Region einzigartig. Weitere Informationen zum Abrufen Ihrer SMTP-Anmeldeinformationen finden Sie unter Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen.

Schritt 5. Herstellen einer Verbindung mit einem SMTP-Endpunkt

Wenn Sie einen Message Transfer Agent wie Postfix oder Sendmail verwenden, müssen Sie die Konfiguration für diese Anwendung aktualisieren, um auf einen Amazon-SES-SMTP-Endpunkt zu verweisen. Eine vollständige Liste der SMTP-Endpunkte finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt. Beachten Sie, dass die SMTP-Anmeldeinformationen, die Sie im vorherigen Schritt erstellt haben, einer bestimmten AWS Region zugeordnet sind. Sie müssen eine Verbindung zum SMTP-Endpunkt in der Region herstellen, in der Sie die SMTP-Anmeldeinformationen erstellt haben.

Nächste Schritte

An diesem Punkt können Sie mit dem Senden von E-Mails mit Amazon SES beginnen. Es gibt jedoch einige optionale Schritte, die Sie durchführen können.

- Sie können Konfigurationssätze erstellen, bei denen es sich um Regelsätze handelt, die auf die von Ihnen gesendeten E-Mail-Nachrichten angewendet werden. Sie können Konfigurationssätze etwa verwenden, um anzugeben, wo Benachrichtigungen gesendet werden, wenn eine E-Mail-Nachricht zugestellt wird, wenn ein Empfänger eine Nachricht öffnet oder auf einen Link klickt, wenn eine E-Mail-Nachricht unzustellbar ist, und wenn ein Empfänger Ihre E-Mail-Nachricht als Spam markiert. Weitere Informationen finden Sie unter Verwenden von Amazon SES-Konfigurationssätzen im.
- Wenn Sie E-Mails über Amazon SES senden, ist es wichtig, die Unzuzuzustellung und Beschwerden für Ihr Konto zu überwachen. Amazon SES enthält eine Konsolenseite für Reputationsmetriken, mit der Sie die Unzuzuzustellung und Beschwerden für Ihr Konto verfolgen können. Weitere Informationen finden Sie unter Verwenden des Reputation Dashboards zum Nachverfolgen von Unzustellbarkeits- und Beschwerdequoten. Sie können auch CloudWatch

Alarme erstellen, die Sie benachrichtigen, wenn diese Raten zu hoch werden. Weitere Informationen zum Erstellen von CloudWatch Alarmen finden Sie unterErstellen von Alarmen zur Reputationsüberwachung mit CloudWatch.

- Kunden, die eine große Menge von E-Mail-Nachrichten senden, oder solche, die einfach nur die volle Kontrolle über die Zuverlässigkeiten ihrer IP-Adressen haben möchten, können dedizierte IP-Adressen gegen eine zusätzliche monatliche Gebühr leasen. Weitere Informationen finden Sie unter Verwenden dedizierter IP-Adressen mit Amazon SES.

Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox)

Um Betrug und Missbrauch zu vermeiden und Ihre Reputation als Absender zu schützen, wenden wir bestimmte Einschränkungen auf neue Amazon SES-Konten an.

Wir platzieren alle neuen Konten in der Amazon SES-Sandbox. Der Sandbox-Status für Ihr Konto ist für jedes Konto einzigartig. AWS-Region Während sich Ihr Konto in der Sandbox befindet, können Sie alle Funktionen von Amazon SES verwenden. Solange sich Ihr Konto in der Sandbox befindet, gelten jedoch die folgenden Einschränkungen für Ihr Konto:

- Sie können E-Mails nur an von Ihnen verifizierte E-Mail-Adressen und Domänen oder an den Amazon SES-Postfachsimulator senden.
- Sie können innerhalb von 24 Stunden nur maximal 200 E-Mails versenden.
- Pro Sekunden kann nur 1 Nachricht verschickt werden.
- Für die Sendeautorisierung können weder Sie noch der stellvertretende Sender E-Mails an nicht verifizierte E-Mail-Adressen senden.
- Für die Unterdrückung auf Kontoebene sind Massenaktionen und SES-API-Aufrufe im Zusammenhang mit der Verwaltung der Unterdrückungsliste deaktiviert.

Wenn Ihr Konto aus der Sandbox in die Produktionsumgebung übergegangen ist, können Sie E-Mails an jeden beliebigen Empfänger senden, unabhängig davon, ob die Adresse oder Domain des Empfängers verifiziert ist. Sie müssen jedoch weiterhin alle Identitäten überprüfen, die Sie als Adressen für „From“ (Von), „Source“ (Quelle), „Sender“ (Absender) oder „Return-Path“ (Rücksendepfad) verwenden.

Gehen Sie wie in diesem Abschnitt beschrieben vor, um zu beantragen, dass Ihr Konto aus der Sandbox entfernt und in Betrieb genommen wird.

> **Tip**
>
> - Wenn Sie ein neuer Kunde sind und noch keine Identitäten erstellt haben, wird der SES-Kontoeinrichtungsassistent in der Konsole aktiviert, um Ihnen den Einstieg zu erleichtern. Anweisungen zum Zugriff auf den Assistenten finden Sie unter Ihr SES-Konto einrichten.
> - Wenn Sie bereits eine oder mehrere Identitäten erstellt haben, wird anstelle des Assistenten für die Kontoeinrichtung die Seite „Einrichtung erstellen“ angezeigt.
>   - Wenn es sich bei einer Ihrer Identitäten um eine verifizierte Domain handelt, können Sie den Produktionszugriff auch direkt von der Seite „Einrichtung abrufen“ aus beantragen. Dies liegt daran, dass es sich bewährt hat, Ihre Domain bei SES zu verifizieren, bevor Sie Produktionszugriff beantragen. So können Sie Ihre Anfrage für Produktionszugriff schneller genehmigen, sodass Sie sofort mit dem Senden von E-Mails beginnen können.

> **Note**
>
> - Wenn Sie Amazon SES verwenden, um E-Mails von einer Amazon-EC2-Instance zu senden, müssen Sie möglicherweise auch anfordern, dass die Drosselung von Port 25 auf Ihrer -Instance entfernt wird. Weitere Informationen finden Sie unter Wie entferne ich die Drosselung an Port 25 aus meiner EC2-Instance? im AWS Knowledge Center.

Um Zugriff auf die Produktion zu beantragen (entfernen Sie Ihr Konto aus der Sandbox), verwenden Sie AWS-Managementkonsole

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich Konto-Dashboard aus.
3. Wählen Sie im Warnfeld oben in der Konsole mit der Aufschrift „Ihr Amazon SES SES-Konto befindet sich in der Sandbox“ auf der rechten Seite die Option Ansicht Seite einrichten und anschließend Produktionszugriff anfordern aus.
4. Wählen Sie im modalen Kontodetails entweder das KontrollkästchenMarketingoderTransaktional, das die meisten E-Mails, die Sie senden, am besten beschreibt.

   - Marketing-E-Mail — Wird auf der one-to-many Grundlage einer gezielten Liste von Interessenten oder Kunden gesendet und enthält Marketing- und Werbeinhalte, z. B. um einen Kauf zu tätigen, Informationen herunterzuladen usw.

- Transaktions-E-Mail — Wird auf einer one-to-one für jeden Empfänger eindeutigen Grundlage gesendet, die normalerweise durch eine Benutzeraktion wie einen Kauf auf der Website, eine Anfrage zum Zurücksetzen des Passworts usw. ausgelöst wird.

5. In Website URL (Website-URL) geben Sie die URL Ihrer Website ein, um uns zu helfen, die Art von Inhalten, die Sie senden möchten, besser zu verstehen.
6. In Additional contacts (Zusätzliche Kontakte) teilen Sie uns mit, wo Sie Mitteilungen über Ihr Konto erhalten möchten. Dies kann eine durch Kommata getrennte Liste mit bis zu 4 E-Mail-Adressen sein.
7. In Preferred contact language (Bevorzugte Kontaktsprache) wählen Sie aus, ob Sie Mitteilungen inEnglisch oder Japanisch möchten.
8. In Acknowledgement (Bestätigung) aktivieren Sie das Kontrollkästchen, dass Sie damit einverstanden sind, E-Mails nur an Personen zu senden, die diese explizit angefordert haben, und bestätigen Sie, dass Sie einen Prozess für die Bearbeitung von Bounce- und Reklamationsbenachrichtigungen eingerichtet haben.
9. Wählen Sie das SymbolSenden von Anfragen- ein Banner wird angezeigt, um zu bestätigen, dass Ihre Anfrage eingereicht wurde und derzeit geprüft wird.

Sobald Sie eine Überprüfung Ihrer Kontodetails eingereicht haben, können Sie Ihre Daten erst bearbeiten, wenn die Überprüfung abgeschlossen ist. Das AWS Support Team gibt innerhalb von 24 Stunden eine erste Antwort auf Ihre Anfrage.

Da wir verhindern möchten, dass unerwünschte oder schädliche Inhalte in unseren Systemen eingehen, müssen wir jede Anfrage sorgfältig prüfen. Nach einer erfolgreichen Prüfung kommen wir Ihrer Anfrage innerhalb dieses 24-Stunden-Zeitraums nach. Für den Fall, dass wir weitere Informationen von Ihnen benötigen, kann die Bearbeitung Ihrer Anfrage länger dauern.

Optional können Sie Ihre Anfrage für den Zugriff auf die Produktion auch über die einreichen AWS CLI. Das Einreichen Ihrer Anfrage über AWS CLI ist hilfreich, wenn Sie Produktionszugriff für eine große Anzahl von Identitäten beantragen oder wenn Sie den Prozess der Einrichtung von Amazon SES automatisieren möchten.

Um zu beantragen, dass Ihr Konto aus der Amazon SES SES-Sandbox entfernt wird, verwenden Sie den AWS CLI

1. VoraussetzungZum Installieren und Konfigurieren des AWS CLI aus. Weitere Informationen finden Sie im AWS Command Line Interface -Benutzerhandbuch.

2. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 put-account-details \
--production-access-enabled \
--mail-type TRANSACTIONAL \
--website-url https://example.com \
--additional-contact-email-addresses info@example.com \
--contact-language EN
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

a. *TRANSACTIONAL*Ersetzen Sie es durch den E-Mail-Typ, den Sie über Amazon SES versenden möchten. Sie können entweder `TRANSACTIONAL` oder `MARKETING` angeben. Wenn mehr als ein Wert zutrifft, wählen Sie die Option aus, die für die meisten der E-Mails gilt, die Sie senden möchten.

b. *https://example.com*Ersetzen Sie es durch die URL Ihrer Website. Durch die Bereitstellung dieser Informationen können wir besser einschätzen, welche Art von Inhalt Sie senden möchten.

c. *info@example.com*Ersetzen Sie es durch die E-Mail-Adressen, an die Sie Mitteilungen zu Ihrem Konto erhalten möchten. Dies kann eine durch Kommata getrennte Liste mit bis zu 4 E-Mail-Adressen sein.

d. Ersetze es *EN* durch deine bevorzugte Sprache. Sie können`EN`Für Englisch oder`JA`Für Japanisch.

Sobald Sie eine Überprüfung Ihrer Kontodetails eingereicht haben, können Sie Ihre Daten erst bearbeiten, wenn die Überprüfung abgeschlossen ist. Das AWS Support Team gibt innerhalb von 24 Stunden eine erste Antwort auf Ihre Anfrage.

Da wir verhindern möchten, dass unerwünschte oder schädliche Inhalte in unseren Systemen eingehen, müssen wir jede Anfrage sorgfältig prüfen. Nach einer erfolgreichen Prüfung kommen wir Ihrer Anfrage innerhalb dieses 24-Stunden-Zeitraums nach. Für den Fall, dass wir weitere Informationen von Ihnen benötigen, kann die Bearbeitung Ihrer Anfrage länger dauern.

Verwalten Ihrer Amazon SES Versandkontingente

Ihr Amazon-SES-Konto verfügt über eine Reihe von Sendekontingenten, um die Anzahl der E-Mail-Nachrichten, die Sie versenden können, und die Rate, mit der Sie sie versenden können, zu regulieren. Die Sendekontingente kommen allen Amazon-SES-Kunden zugute, da sie dazu beitragen, die Vertrauensstellung zwischen Amazon SES und E-Mail-Anbietern aufrechtzuerhalten. Sendekontingente helfen Ihnen dabei, Ihre Sendeaktivität allmählich zu steigern und die Wahrscheinlichkeit zu verringern, dass E-Mail-Anbieter Ihre E-Mails wegen plötzlicher, unerwarteter Spitzen in Ihrem E-Mail-Volumen oder der Senderate blockieren.

Die folgenden Kontingente gelten für das Senden von E-Mails über Amazon SES:

- Sendequote – Die maximale Anzahl an E-Mails, die Sie in 24 Stunden senden können. Dieses Kontingent wird für einen gleitenden Zeitraum berechnet. Jedes Mal, wenn Sie versuchen, eine E-Mail zu senden, ermittelt Amazon SES die Anzahl der E-Mails, die Sie in den letzten 24 Stunden gesendet haben. Solange die Gesamtzahl der E-Mails, die Sie in den letzten 24 Stunden gesendet haben, unter diesem täglichen Maximum liegt, wird Ihre Sendeanforderung akzeptiert und Ihre E-Mail gesendet.

  Wenn das Senden einer Nachricht das tägliche Maximum für Ihr Konto überschreiten würde, wird der Aufruf an Amazon SES abgelehnt.
- Maximale Senderate - die maximale Anzahl an E-Mails, die Amazon SES pro Sekunde von Ihrem Konto akzeptieren kann. Sie können dieses Kontingent für kurze Spitzenphasen überschreiten, jedoch nicht für einen längeren Zeitraum.

  > **Note**
  >
  > Die Rate, mit der Amazon SES Ihre Nachrichten akzeptiert, kann niedriger sein als die maximale Senderate für Ihr Konto.
- Maximale Nachrichtengröße (MB): Die maximale E-Mail-Größe, die Sie senden können. Dies schließt alle Bilder und Anhänge ein, die nach der MIME-Codierung Teil der E-Mail sind. Wenn Sie beispielsweise eine Datei mit 5 MB anhängen, beträgt die Größe der Anlage in der E-Mail nach der MIME-Codierung ~ 6,85 MB (etwa 137% der ursprünglichen Dateigröße).

> **Note**
>
> Wir empfehlen Ihnen, Ihre Anhänge auf Cloud-Laufwerke hochzuladen und die URL des Cloud-Laufwerks anzugeben, um die E-Mail-Größe zu reduzieren und die Zustellbarkeit zu verbessern. SES kann nicht garantieren, dass große E-Mails im Empfängerpostfach landen, da verschiedene Mail-Server über unterschiedliche Größenrichtlinien verfügen.

Ihre Amazon SES SES-Sendekontingente sind für jede AWS Region separat. Informationen zur Verwendung von Amazon SES in mehreren AWS Regionen finden Sie unterRegionen und Amazon SES.

Wenn sich Ihr Konto in der Amazon-SES-Sandbox befindet, können Sie nur 200 Nachrichten pro 24-Stunden-Zeitraum senden und Ihre maximale Senderate beträgt eine Nachricht pro Sekunde. Wenn Sie die Entfernung Ihres Kontos aus der Sandbox anfordern, können Sie auch gleichzeitig eine Erhöhung Ihrer Kontingente anfordern. Weitere Informationen darüber, wie Ihr Konto aus der Sandbox entfernt werden kann, finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox)

Wenn Ihr Konto aus der Sandbox entfernt wurde, können Sie jederzeit zusätzliche Kontingenterhöhungen beantragen, indem Sie im AWS Support Center einen neuen Fall erstellen. Weitere Informationen finden Sie unter Erhöhen Ihrer Amazon-SES-Sendekontingente.

> **Note**
>
> Sendekontingente beziehen sich auf die Anzahl der Empfänger, nicht der Nachrichten. Z. B. zählt eine E-Mail mit 10 Empfängern bei der Quote als 10. Wir raten Ihnen jedoch davon ab, eine E-Mail an mehrere Empfänger in einem einzigen Aufruf der `SendEmail`-API-Operation zu senden, da mit einem Fehlschlagen des Aufrufs die gesamte E-Mail zurückgewiesen wird. Wir empfehlen Ihnen, für jeden Empfänger einmal `SendEmail` aufzurufen.

- Informationen zum Erhöhen der Sendekontingente finden Sie unter Erhöhen Ihrer Amazon-SES-Sendekontingente.
- Informationen dazu, wie Sie Ihre Sendekontingente mithilfe der Amazon-SES-Konsole oder der Amazon-SES-API überwachen, finden Sie unter Überwachung Ihrer Amazon-SES-Sendekontingente.

- Informationen zu den Fehlern, die Ihre Anwendung bei Erreichen der Sendekontingente erhält, finden Sie unter Fehler im Zusammenhang mit Sendekontingenten für Ihr Amazon-SES-Konto.

Erhöhen Ihrer Amazon-SES-Sendekontingente

Ihr Konto umfasst die folgenden Kontingente pro Ihrer aktuellen Region.

Ressource	Standardkontingent	Description
Sendequote	200	Die maximale Anzahl von E-Mails, die Sie in einem Zeitraum von 24 Stunden für dieses Konto im aktuellen AWS-Region senden können.
Senderate	1	Die maximale Anzahl von E-Mails, die Amazon SES pro Sekunde für dieses Konto in der aktuellen AWS-Region annehmen kann.

Automatisch erhöhte Sendekontingente

Wenn sich Ihr Konto außerhalb der Sandbox befindet und Sie qualitativ hochwertige Produktions-E-Mails senden, erhöhen wir das Sendekontingente für Ihr Konto möglicherweise automatisch. Oft erhöhen wir diese Kontingente automatisch, bevor Sie sie tatsächlich erhöhen müssen.

Wenn Sie automatische Ratenerhöhungen erhalten möchten, müssen alle der folgenden Aussagen wahr sein:

- Sie senden hochwertige Inhalte, die Ihre Empfänger erhalten möchten – Sie Senden Inhalte, die von den Empfängern erwünscht und erwartet werden. Sie senden Kunden, die Ihre E-Mails nicht öffnen, keine weiteren E-Mails mehr.
- Sie senden tatsächliche Produktionsinhalte - Das Senden von Testnachrichten an gefälschte E-Mail-Adressen kann sich negativ auf Ihre Unzustellbarkeits- und Beschwerdequoten auswirken. Wenn Sie außerdem Nachrichten nur an interne Empfänger senden, lässt sich nur schwer feststellen, ob Sie Inhalte versenden, die Ihre Kunden erhalten möchten. Wenn Sie Ihre Produktionsnachrichten allerdings an externe Empfänger senden, können wir Ihr E-Mail-Sendeverhalten genau einschätzen.

- Sie nutzen Ihr aktuelles Kontingent fast voll aus - Um sich für eine automatische Kontingenterhöhung zu qualifizieren, sollte sich Ihr tägliches E-Mail-Volumen regelmäßig dem täglichen Maximum für Ihr Konto nähern, ohne es zu überschreiten.
- Sie haben niedrige Unzustellbarkeits- und Beschwerderaten - Verringern Sie die Anzahl der unzustellbaren E-Mails und der erhaltenen Beschwerden. Eine hohe Anzahl von unzustellbaren E-Mails und Beschwerden kann sich negativ auf Ihre Sendekontingente auswirken.

Benutzer angefordert erhöhte Sendequoten

Wenn Ihre aktuellen Sendekontingente Ihren Bedürfnissen nicht entsprechen und wir die Kontingente nicht automatisch erhöhen, können Sie eine Erhöhung anfordern:

- Sendequote oder Senderate – Anforderungen zur Erhöhung einer dieser beiden Werte können über die AWS Service Quotas-Konsole gestellt werden.

So fordern Sie eine Erhöhung Ihrer Amazon SES an, indem Sie Kontingente über die Service Quotas ente-Konsole senden.

1. Öffnen Sie die Service Quotas console (Service-Quotas-Konsole).
2. Wählen Sie die Region aus, für die die Erhöhung erfolgen soll, indem Sie das Dropdown-Menü in der oberen rechten Ecke der Konsole (neben Ihrer Kontonummer) verwenden.
3. Wählen Sie im Navigationsbereich AWS -Services.
4. Wählen Sie Amazon Simple Email Service (SES).
5. Wählen Sie ein Kontingent aus, und folgen Sie den Anweisungen, um eine Kontingenterhöhung anzufordern.

> **AWS Support Team-SLA für erhöhte Anforderungstypen**
>
> Da wir verhindern möchten, dass unerwünschte oder schädliche Inhalte in unseren Systemen eingehen, müssen wir jede Anfrage sorgfältig prüfen. Wenn wir dies tun können, kommen wir Ihrer Anfrage innerhalb der unten aufgeführten Zeiten für die Art der beantragten Erhöhung nach. Für den Fall, dass wir weitere Informationen von Ihnen benötigen, kann die Bearbeitung Ihrer Anfrage länger dauern. Wir behalten uns das Recht vor, Ihrer Anfrage nicht stattzugeben, wenn Ihr Anwendungsfall nicht mit unseren Richtlinien übereinstimmt.

- Sendequote oder Senderate: Bis zu 24 Stunden.

> **Note**
>
> Während die Service Quotas Konsole in vielen verschiedenen Sprachen verfügbar ist, wird der eigentliche Support nur in Englisch angeboten.

Überwachung Ihrer Amazon-SES-Sendekontingente

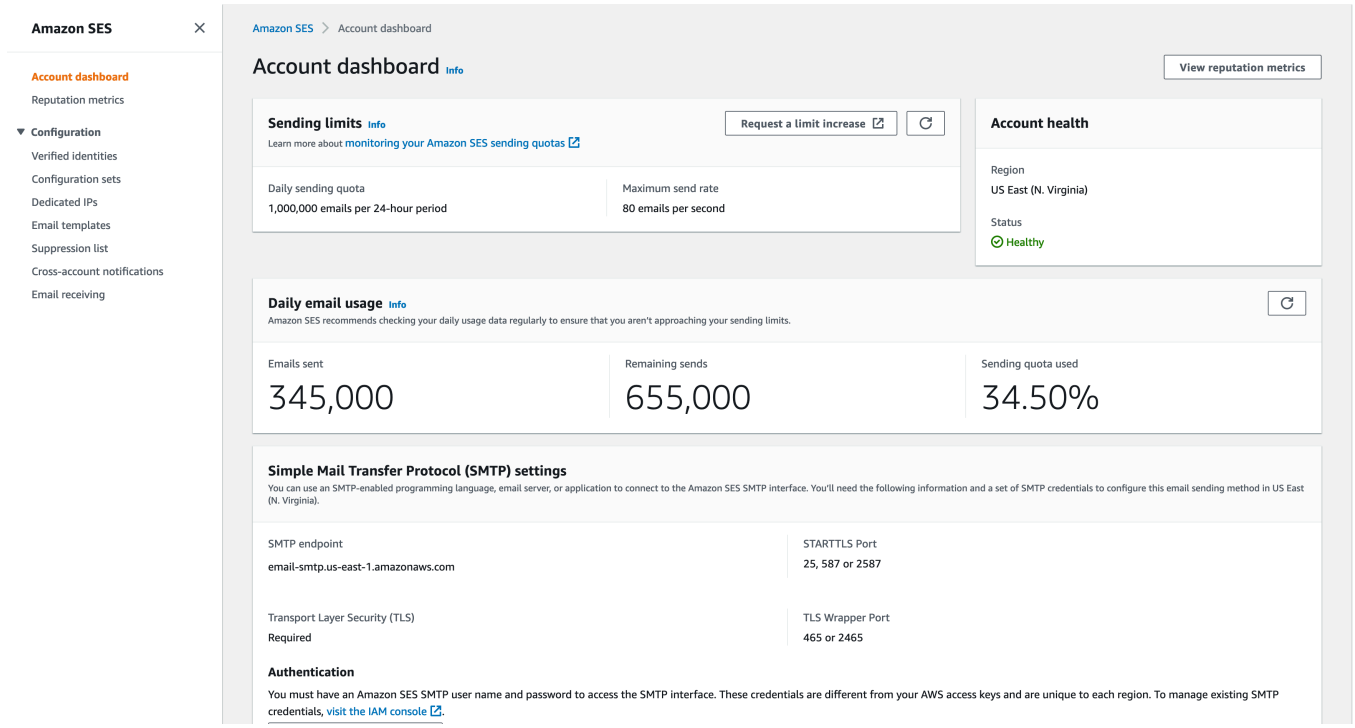
Sie können Ihre Sendekontingente mit Hilfe der Amazon-SES-Konsole oder über die Amazon-SES-API überwachen – durch den direkten oder indirekten Aufruf der Abfragen-(HTTPS)-Schnittstelle über ein AWS -SDK, AWS Command Line Interface oder AWS Tools for Windows PowerShell.

> **Important**
>
> Wir empfehlen Ihnen, Ihre Sendestatistiken regelmäßig zu überprüfen. So stellen Sie sicher, dass Sie sich nicht der Grenze Ihrer Sendekontingente annähern. Wenn Sie sich an der Grenze zu Ihren Sendekontingenten befinden, finden Sie unter Erhöhen Ihrer Amazon-SES-Sendekontingente Informationen darüber, wie Sie diese erhöhen können. Warten Sie nicht, bis Sie die Grenze Ihrer Sendekontingente erreicht haben, um eine Erhöhung in Betracht zu ziehen.

Überwachung Ihrer Sendekontingente mithilfe der Amazon-SES-Konsole

Die folgende Vorgehensweise zeigt Ihnen, wie Sie Ihre Sendekontingente mithilfe der Amazon-SES-Konsole anzeigen können.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard) aus. Ihre Sendekontingente werden unter Your Amazon SES Sending Limits (Ihre Sendelimits für Amazon SES) angezeigt. Die Gesamtzahl der gesendeten E-Mails, der verbleibenden E-Mails und der Prozentsatz der verwendeten Sendequote wird unter Daily email usage (Tägliche E-Mail-Nutzung) angezeigt.



3. Um die Anzeige zu aktualisieren, wählen Sie in der oberen rechten Ecke desTägliche E-Mail-Nutzungaus.

Überwachung Ihrer Sendekontingente mithilfe der Amazon-SES-API

Die Amazon-SES-API stellt die `GetSendQuota`-Aktion zur Verfügung, die Ihre Sendekontingente zurückgibt. Wenn Sie die `GetSendQuota`-Aktion aufrufen, erhalten Sie die folgenden Informationen:

- Anzahl der E-Mails, die Sie in den letzten 24 Stunden versendet haben
- Sendequote für den aktuellen 24-Stunden-Zeitraum
- Maximale Senderate

> **Note**
>
> Eine Beschreibung von `GetSendQuota` finden Sie unter Amazon Simple Email Service API-Referenz.

Fehler im Zusammenhang mit Sendekontingenten für Ihr Amazon-SES-Konto

Wenn Sie eine E-Mail senden, nachdem Sie Ihre tägliche Sendequote (die maximale Anzahl von E-Mails, die Sie in 24 Stunden senden können) oder Ihre maximale Senderate (die maximale Anzahl von Nachrichten, die pro Sekunde gesendet werden können) erreicht haben, löscht Amazon SES die Nachricht und versucht nicht, sie erneut zuzustellen. Amazon SES stellt auch eine Fehlermeldung bereit, die das Problem erklärt. Die Art und Weise, wie Amazon SES diese Fehlermeldung erzeugt, hängt davon ab, wie Sie die E-Mail senden wollten. Dieses Thema enthält Informationen zu den Nachrichten, die Sie über die Amazon-SES-API und die SMTP-Schnittstelle erhalten.

Eine verwendbare Technik beim Erreichen Ihrer maximalen Senderate finden Sie unter How to handle a „Throttling – Maximum sending rate exceeded“ error im AWS Messaging- und Targeting-Blog.

Erreichen von Sendelimits mit der Amazon-SES-API

Wenn Sie versuchen, eine E-Mail mithilfe der Amazon SES SES-API (oder eines AWS SDK) zu senden, aber die Sendelimits Ihres Kontos bereits überschritten haben, gibt die API einen `ThrottlingException` Fehler aus. Die Fehlermeldung enthält eine der folgenden Meldungen:

- `Daily message quota exceeded`
- `Maximum sending rate exceeded`

Wenn ein Drosselungsfehler auftritt, sollten Sie Ihre Anwendung so programmieren, dass sie für einen Zeitraum von bis zu 10 Minuten wartet, und versuchen Sie dann erneut, die Sendeanforderung zu senden.

Erreichen von Sendelimits mit SMTP

Wenn Sie versuchen, eine E-Mail über die Amazon-SES-SMTP-Schnittstelle zu senden, Sie aber bereits die Sendelimits Ihres Kontos überschritten haben, zeigt Ihr SMTP-Client möglicherweise einen der folgenden Fehler an:

- `454 Throttling failure: Maximum sending rate exceeded`
- `454 Throttling failure: Daily message quota exceeded`

Verschiedene SMTP-Clients behandeln diese Fehler auf unterschiedliche Weise.

Einrichten von E-Mail mit Amazon SES

Sie können eine E-Mail mit Amazon Simple Email Service (Amazon SES) über die Amazon SES), die Amazon SES Simple Mail Transfer Protocol (SMTP) -Schnittstelle oder die Amazon SES -API senden. Normalerweise wird die Konsole zum Senden von Test-E-Mails und zum Verwalten Ihrer Sendeaktivität verwendet. Zum Senden von Massen-E-Mails verwenden Sie entweder die SMTP-Schnittstelle oder die API. Weitere Informationen zu den Amazon-SES-E-Mail-Preisen erhalten Sie unter Amazon SES Preise.

- Wenn Sie ein SMTP-fähiges Softwarepaket, eine Anwendung oder eine Programmiersprache verwenden möchten, um E-Mails über Amazon SES zu senden oder Amazon SES in Ihren vorhandenen E-Mail-Server zu integrieren, verwenden Sie die Amazon-SES-SMTP-Schnittstelle. Weitere Informationen finden Sie unter Programmatisches Senden einer E-Mail über die Amazon-SES-SMTP-Schnittstelle.
- Wenn Sie Amazon SES über unformatierte HTTP-Anforderungen aufrufen möchten, verwenden Sie die Amazon-SES-API. Weitere Informationen finden Sie unter Verwenden der Amazon-SES-API zum Senden von E-Mails.

> **Important**
>
> Wenn Sie eine E-Mail an mehrere Empfänger senden („To“-, „CC“- und „BCC“-Adressen) und der Aufruf an Amazon SES fehlschlägt, wird die gesamte E-Mail abgelehnt und keiner der Empfänger enthält die beabsichtigte E-Mail. Wir empfehlen daher, dass Sie eine E-Mail nur jeweils an einen Empfänger senden.

Verwenden der Amazon-SES-SMTP-Schnittstelle zum Senden von E-Mails

Sie können die Simple Mail Transfer Protocol(SMTP)-Schnittstelle oder die Amazon SES-API verwenden, um Produktions-E-Mails über Amazon SES zu senden. Weitere Informationen zur Amazon-SES-API finden Sie unter Verwenden der Amazon-SES-API zum Senden von E-Mails. In diesem Abschnitt wird die SMTP-Schnittstelle beschrieben.

Amazon SES sendet E-Mails über SMTP, dem gängigsten E-Mail-Protokoll im Internet. Sie können E-Mails über Amazon SES senden, indem Sie eine Vielzahl von SMTP-fähigen Programmiersprachen

und SMTP-fähiger Software verwenden, um eine Verbindung zur Amazon-SES-SMTP-Schnittstelle herzustellen. In diesem Abschnitt wird erklärt, wie Sie Ihre Amazon-SES-SMTP-Anmeldeinformationen abrufen, wie Sie mithilfe der SMTP-Schnittstelle E-Mails versenden und wie Sie mehrere Softwarebestandteile und E-Mail-Server für den E-Mail-Versand über Amazon SES konfigurieren.

Lösungen für häufige Probleme, die auftreten können, wenn Sie Amazon SES über die SMTP-Schnittstelle verwenden, finden Sie unter SMTP-Probleme bei Amazon SES.

Anforderungen zum Senden von E-Mails über SMTP

Zum Senden von E-Mails über die Amazon-SES-SMTP-Schnittstelle benötigen Sie Folgendes:

- Die SMTP-Endpunktadresse. Eine Liste der Amazon SES SMTP-Endpunkte finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt.
- Portnummer der SMTP-Schnittstelle. Die Portnummer variiert je nach Verbindungsmethode. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt.
- Ein SMTP-Benutzername und -Passwort. SMTP-Anmeldeinformationen sind für jede AWS -Region eindeutig. Wenn Sie die SMTP-Schnittstelle verwenden möchten, um E-Mails in mehreren AWS -Regionen zu senden, benötigen Sie SMTP-Anmeldeinformationen für jede Region.

  > **Important**
  >
  > Ihre SMTP-Anmeldeinformationen sind nicht identisch mit Ihren AWS Zugangsschlüsseln oder den Anmeldeinformationen, mit denen Sie sich bei der Amazon SES-Konsole anmelden. Weitere Informationen zum Generieren von SMTP-Anmeldeinformationen finden Sie unter Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen.

- Client-Software, die mithilfe von Transport Layer Security (TLS) kommunizieren kann. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt.
- Eine E-Mail-Adresse, die Sie mit Amazon SES überprüft haben. Weitere Informationen finden Sie unter Verifizierte Identitäten in Amazon SES.
- Höhere Sendekontingente, wenn Sie große Mengen E-Mails senden möchten. Weitere Informationen finden Sie unter Verwalten Ihrer Amazon SES Versandkontingente.

Methoden zum Senden von E-Mails über SMTP

Sie können E-Mails über SMTP mit einer der folgenden Methoden senden:

- Weitere Informationen zur Konfiguration SMTP-fähiger Software für das Senden von E-Mails über die Amazon SES-SMTP-Schnittstelle finden Sie unter Senden von E-Mails über Amazon SES mithilfe von Softwarepaketen.
- Informationen zum Programmieren einer Anwendung für das Senden von E-Mails über Amazon SES finden Sie unter Programmatisches Senden einer E-Mail über die Amazon-SES-SMTP-Schnittstelle.
- Informationen zum Konfigurieren Ihres bestehenden E-Mail-Servers für das Senden aller ausgehenden E-Mails über Amazon SES finden Sie unter Integrieren von Amazon SES in Ihren vorhandenen E-Mail-Server.
- Informationen zur Interaktion mit der Amazon SES-SMTP-Schnittstelle über die Befehlszeile, was nützlich für Tests sein kann, finden Sie unter Testen der Verbindung zur Amazon-SES-SMTP-Schnittstelle über die Befehlszeile.

Eine Liste der SMTP-Antwort-Codes finden Sie unter Von Amazon SES zurückgegebene SMTP-Antwortcodes.

Anzugebende E-Mail-Informationen

Wenn Sie über die SMTP-Schnittstelle auf Amazon SES zugreifen, erstellt Ihre SMTP-Clientanwendung die Nachricht. Daher hängen die Informationen, die Sie bereitstellen müssen, von der verwendeten Anwendung ab. Für den SMTP-Datenaustausch zwischen einem Client und einem Server sind mindestens Folgendes erforderlich:

- Quell-IP-Adresse
- Zieladresse
- Nachrichten-Tags

Wenn Sie die SMTP-Schnittstelle verwenden und die Weiterleitung von Feedback aktiviert ist, werden die Unzustellbaren E-Mails, Beschwerden und Zustellungsbenachrichtigungen an die „MAIL FROM“-Adresse gesendet. Es wird keine der von Ihnen angegebenen „Reply-To“-Adressen verwendet.

Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen

Sie benötigen SMTP-Anmeldeinformationen für Amazon SES, um auf die SES-SMTP-Schnittstelle zugreifen zu können.

Die Anmeldeinformationen, die Sie zum Senden von E-Mails über die SES SMTP-Schnittstelle verwenden, sind für jede AWS Region einzigartig. Wenn Sie die SES-SMTP-Schnittstelle zum Senden von E-Mails in mehr als einer Region verwenden, müssen Sie einen Satz von SMTP-Anmeldeinformationen für jede Region erstellen.

Ihr SMTP-Passwort unterscheidet sich von Ihrem AWS geheimen Zugangsschlüssel. Weitere Informationen zu Anmeldeinformationen finden Sie unter Arten von Amazon-SES-Anmeldeinformationen.

> **Note**
>
> Eine Liste der derzeit verfügbaren SMTP-Endpunkte finden Sie unter SMTP-Endpunkte in der. Allgemeine AWS-Referenz

Abrufen der SES-SMTP-Anmeldeinformationen über die SES-Konsole

Anforderung

Ein IAM-Benutzer kann SES-SMTP-Anmeldeinformationen erstellen, die Richtlinie des Benutzers muss diesen jedoch die Berechtigung zur Nutzung von IAM selbst erteilen, da die SES-SMTP-Anmeldeinformationen mit IAM erstellt werden. Ihre IAM-Richtlinie muss es Ihnen ermöglichen, die folgenden IAM-Aktionen durchzuführen:`iam:CreateUser`,,, und. `iam:CreateGroup` `iam:PutGroupPolicy` `iam:AddUserToGroup` `iam:CreateAccessKey` Wenn Sie versuchen, SES-SMTP-Anmeldeinformationen mithilfe der Konsole zu erstellen, und Ihr IAM-Benutzer nicht über diese Berechtigungen verfügt, wird möglicherweise ein Fehler angezeigt, oder die SMTP-Anmeldeinformationen wurden möglicherweise ohne die richtigen Richtlinieneinstellungen erstellt.

> **Important**
>
> Einige der oben genannten IAM-Aktionen, insbesondere `iam:PutGroupPolicy` und`iam:AddUserToGroup`, haben die Zugriffsebene Permission Management, die höchste IAM-Stufe, da sie die Erlaubnis erteilt, Ressourcenberechtigungen im Service zu erteilen oder zu ändern. Um die Sicherheit Ihres AWS Kontos zu verbessern, wird daher dringend

empfohlen, diese Richtlinien, zu denen auch die Zugriffsebenenklassifizierung für die Berechtigungsverwaltung gehört, einzuschränken oder regelmäßig zu überwachen.

So erstellen Sie Ihre SMTP-Anmeldeinformationen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie SMTP-Einstellungen im linken Navigationsbereich aus. Dadurch wird die Seite Simple Mail Transfer Protocol (SMTP) settings (Einstellungen für Simple Mail Transfer Protocol (SMTP) geöffnet.
3. Wählen Sie Create SMTP Credentials (SMTP-Anmeldeinformationen erstellen) aus. In der oberen rechten Ecke wird die IAM-Konsole geöffnet.
4. (Optional) Wenn Sie bereits erstellte SMTP-Benutzer anzeigen, bearbeiten oder löschen müssen, wählen Sie unten rechts Manage my existing SMTP credentials (Meine vorhandenen SMTP-Zugangsdaten verwalten) aus. Die IAM-Konsole wird geöffnet. Details zum Verwalten von SMTP-Anmeldeinformationen werden nach diesen Verfahren angegeben.
5. Geben Sie für Benutzer für SMTP erstellen einen Namen für Ihren SMTP-Benutzer in das Feld Benutzername ein. Alternativ können Sie den Standardwert verwenden, der in diesem Feld bereitgestellt wird. Wenn Sie fertig sind, wählen Sie Erstellen in der unteren rechten Ecke.
6. Wählen Sie Anzeigen unter SMTP-Passwort – Ihre SMTP-Anmeldeinformationen werden auf dem Bildschirm angezeigt.
7. Laden Sie diese Anmeldeinformationen herunter, indem Sie CSV-Datei herunterladen auswählen, oder kopieren Sie sie und speichern Sie sie an einem sicheren Ort, da Sie Ihre Anmeldeinformationen nach dem Schließen dieses Dialogfelds nicht anzeigen oder speichern können.
8. Wählen Sie Zurück zur SES-Konsole aus.

Sie können eine Liste der SMTP-Anmeldeinformationen anzeigen, die Sie mit diesem Verfahren erstellt haben. Wählen Sie dazu in der IAM-Konsole unter Access management (Zugriffsverwaltung) die Option Users (Benutzer) aus und suchen Sie über die Suchleiste nach allen Benutzern, denen Sie SMTP-Anmeldeinformationen zugewiesen haben.

Sie können die IAM-Konsole auch verwenden, um vorhandene SMTP-Benutzer zu löschen. Weitere Informationen zum Löschen von Benutzern finden Sie unter Verwalten von IAM-Benutzern im IAM – Handbuch „Erste Schritte“.

Wenn Sie Ihr SMTP-Passwort ändern möchten, löschen Sie Ihren vorhandenen SMTP-Benutzer in der IAM-Konsole. Führen Sie anschließend die oben beschriebenen Schritte aus, um einen neuen Satz von SMTP-Anmeldeinformationen zu generieren.

Abrufen von SES-SMTP-Anmeldeinformationen durch Konvertierung vorhandener AWS Anmeldeinformationen

Wenn Sie einen Benutzer haben, den Sie über die IAM-Schnittstelle eingerichtet haben, können Sie die SES-SMTP-Anmeldeinformationen des Benutzers aus seinen Anmeldeinformationen ableiten. AWS

> **Important**
>
> Verwenden Sie keine temporären AWS Anmeldeinformationen, um SMTP-Anmeldeinformationen abzuleiten. Die SES-SMTP-Schnittstelle unterstützt keine SMTP-Anmeldeinformationen, die von temporären Sicherheitsanmeldeinformationen generiert wurden.

Um dem IAM-Benutzer das Senden von E-Mails über die SES SMTP-Schnittstelle zu ermöglichen

1. Leiten Sie die SMTP-Anmeldeinformationen des Benutzers anhand seiner AWS Anmeldeinformationen ab, indem Sie den in diesem Abschnitt bereitgestellten Algorithmus verwenden und dabei die folgenden Verfahren befolgen.

   Da Sie mit AWS Anmeldeinformationen beginnen, entspricht der SMTP-Benutzername der AWS Zugriffsschlüssel-ID, sodass Sie nur das SMTP-Passwort generieren müssen.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
3. Wählen Sie unter Zugriffsverwaltung die Option Richtlinien und anschließend Richtlinie erstellen aus.
4. Wählen Sie im Richtlinieneditor JSON aus und entfernen Sie jeglichen Beispielcode im Editor.
5. Fügen Sie die folgende Berechtigungsrichtlinie in den Editor ein:

   JSON

```
{
"Version":"2012-10-17",
```

```
    "Statement": [
        {
"Effect": "Allow",
            "Action": "ses:SendRawEmail",
            "Resource": "*"
        }
    ]
}
```

6. Wählen Sie Weiter aus und geben Sie `AmazonSesSendingAccess` in das Feld Richtlinienname gefolgt von Richtlinie erstellen ein.
7. Wählen Sie unter Zugriffsverwaltung die Option Benutzergruppen und anschließend Gruppe erstellen aus.
8. Geben Sie `AWSSESSendingGroupDoNotRename` in das Feld Benutzergruppenname ein.
9. Fügen Sie der Gruppe SMTP-Benutzer hinzu, indem Sie sie aus der Tabelle Benutzer zur Gruppe hinzufügen auswählen.
10. Hängen Sie die zuvor erstellte `AmazonSesSendingAccess` Richtlinie an, indem Sie sie aus der Tabelle mit den Richtlinien für Zugriffsrechte anhängen und anschließend Benutzergruppe erstellen auswählen.

Weitere Informationen zur Verwendung von SES mit IAM finden Sie unter Identity and Access Management in Amazon S3.

> **Note**
>
> Sie können zwar SES-SMTP-Anmeldeinformationen für alle IAM-Benutzer generieren, allerdings empfehlen wir, bei der Generierung Ihrer SMTP-Anmeldeinformationen einen separaten IAM-Benutzer zu erstellen. Weitere Informationen zu bewährten Methoden bei der Erstellung von Benutzern für bestimmte Zwecke gehen Sie zu Bewährte Methoden für IAM.

Der folgende Pseudocode zeigt den Algorithmus, der einen AWS geheimen Zugriffsschlüssel in ein SES SMTP-Passwort umwandelt.

```
// Modify this variable to include your AWS secret access key
key = "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY";

// Modify this variable to refer to the AWS Region that you want to use to send email.
region = "us-west-2";
```

```
// The values of the following variables should always stay the same.
date = "11111111";
service = "ses";
terminal = "aws4_request";
message = "SendRawEmail";
version = 0x04;

kDate = HmacSha256(date, "AWS4" + key);
kRegion = HmacSha256(region, kDate);
kService = HmacSha256(service, kRegion);
kTerminal = HmacSha256(terminal, kService);
kMessage = HmacSha256(message, kTerminal);
signatureAndVersion = Concatenate(version, kMessage);
smtpPassword = Base64(signatureAndVersion);
```

Einige Programmiersprachen enthalten Bibliotheken, die Sie verwenden können, um einen geheimen IAM-Zugriffsschlüssel in ein SMTP-Passwort zu konvertieren. Dieser Abschnitt enthält ein Codebeispiel, mit dem Sie mithilfe von Python einen AWS geheimen Zugriffsschlüssel in ein SES-SMTP-Passwort konvertieren können.

> **Note**
>
> - Im folgenden Beispiel werden f-Zeichenfolgen verwendet, die in Python 3.6 eingeführt wurden. Wenn Sie eine ältere Version verwenden, funktionieren sie nicht.
> - Im folgenden Beispiel ist die Liste von SMTP_REGIONS lediglich ein Beispiel. Ihre tatsächliche Liste der Regionen kann kürzer oder länger sein, je nachdem, in welche Regionen Sie E-Mails senden möchten, da Sie für jede Region SMTP-Anmeldeinformationen benötigen. AWS-Region

Python

```
#!/usr/bin/env python3

import hmac
import hashlib
import base64
import argparse
```

```
SMTP_REGIONS = [
    "us-east-2",  # US East (Ohio)
    "us-east-1",  # US East (N. Virginia)
    "us-west-2",  # US West (Oregon)
    "ap-south-1",  # Asia Pacific (Mumbai)
    "ap-northeast-2",  # Asia Pacific (Seoul)
    "ap-southeast-1",  # Asia Pacific (Singapore)
    "ap-southeast-2",  # Asia Pacific (Sydney)
    "ap-northeast-1",  # Asia Pacific (Tokyo)
    "ca-central-1",  # Canada (Central)
    "eu-central-1",  # Europe (Frankfurt)
    "eu-west-1",  # Europe (Ireland)
    "eu-west-2",  # Europe (London)
    "eu-south-1",  # Europe (Milan)
    "eu-north-1",  # Europe (Stockholm)
    "sa-east-1",  # South America (Sao Paulo)
    "us-gov-west-1",  # AWS GovCloud (US)
    "us-gov-east-1",  # AWS GovCloud (US)
]

# These values are required to calculate the signature. Do not change them.
DATE = "11111111"
SERVICE = "ses"
MESSAGE = "SendRawEmail"
TERMINAL = "aws4_request"
VERSION = 0x04


def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()


def calculate_key(secret_access_key, region):
    if region not in SMTP_REGIONS:
        raise ValueError(f"The {region} Region doesn't have an SMTP endpoint.")

    signature = sign(("AWS4" + secret_access_key).encode("utf-8"), DATE)
    signature = sign(signature, region)
    signature = sign(signature, SERVICE)
    signature = sign(signature, TERMINAL)
    signature = sign(signature, MESSAGE)
    signature_and_version = bytes([VERSION]) + signature
    smtp_password = base64.b64encode(signature_and_version)
    return smtp_password.decode("utf-8")
```

```
def main():
    parser = argparse.ArgumentParser(
        description="Convert a Secret Access Key to an SMTP password."
    )
    parser.add_argument("secret", help="The Secret Access Key to convert.")
    parser.add_argument(
        "region",
        help="The AWS Region where the SMTP password will be used.",
        choices=SMTP_REGIONS,
    )
    args = parser.parse_args()
    print(calculate_key(args.secret, args.region))


if __name__ == "__main__":
    main()
```

Um Ihr SMTP-Kennwort mithilfe dieses Skripts zu erhalten, speichern Sie den vorhergehenden Code als `smtp_credentials_generate.py`. Führen Sie in der Befehlszeile den folgenden Befehl aus.

```
python path/to/smtp_credentials_generate.py wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY us-east-1
```

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- Ersetzen Sie es durch den Pfad zu *path/to/* dem Speicherort, an dem Sie gespeichert haben. `smtp_credentials_generate.py`
- *wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY*Ersetzen Sie ihn durch den geheimen Zugriffsschlüssel, den Sie in ein SMTP-Passwort konvertieren möchten.
- *us-east-1*Ersetzen Sie es durch die AWS Region, in der Sie die SMTP-Anmeldeinformationen verwenden möchten.

Wenn dieses Skript erfolgreich ausgeführt wird, ist die einzige Ausgabe Ihr SMTP-Kennwort.

Migrieren eines SMTP-Benutzers von einer vorhandenen Inline-Richtlinie zu einer Gruppenrichtlinie (Sicherheitsempfehlung)

> **Important**
>
> Wenn Sie vor dem 6. September 2024 die SES-SMTP-Anmeldeinformationen erstellt haben, wurden Ihrem SMTP-Benutzer eine Inline-Richtlinie und ein Tag zugewiesen. SES entfernt sich von Inline-Richtlinien und empfiehlt Ihnen als Sicherheitsempfehlung, dasselbe zu tun.

Bevor Sie einen SMTP-Benutzer von einer bestehenden Inline-Richtlinie zu einer Gruppenrichtlinie migrieren, müssen Sie zunächst eine IAM-Benutzergruppe mit der SES-Berechtigungsrichtlinie erstellen, die die Inline-Richtlinie ersetzt. Wenn Sie diese IAM-Benutzergruppe bereits erstellt haben oder wenn sie automatisch für SMTP-Anmeldeinformationen erstellt wurde, die Sie ab dem 6. September 2024 erstellt haben, können Sie in den folgenden Verfahren direkt mit Schritt 10 fortfahren.

So migrieren Sie von einer vorhandenen Inline-Richtlinie zu einer verwalteten Gruppe

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie unter Zugriffsverwaltung die Option Richtlinien und anschließend Richtlinie erstellen aus.
3. Wählen Sie im Richtlinieneditor JSON aus und entfernen Sie jeglichen Beispielcode im Editor.
4. Fügen Sie die folgende Berechtigungsrichtlinie in den Editor ein:

   JSON

```
{
"Version":"2012-10-17",
    "Statement": [
        {
"Effect": "Allow",
            "Action": "ses:SendRawEmail",
            "Resource": "*"
        }
    ]
}
```

5. Wählen Sie Weiter aus und geben Sie `AmazonSesSendingAccess` in das Feld Richtlinienname gefolgt von Richtlinie erstellen ein.
6. Wählen Sie unter Zugriffsverwaltung die Option Benutzergruppen und anschließend Gruppe erstellen aus.
7. Geben Sie `AWSSESSendingGroupDoNotRename` in das Feld Benutzergruppenname ein.
8. Fügen Sie der Gruppe SMTP-Benutzer hinzu, indem Sie sie aus der Tabelle Benutzer zur Gruppe hinzufügen auswählen.
9. Hängen Sie die zuvor erstellte `AmazonSesSendingAccess` Richtlinie an, indem Sie sie aus der Tabelle mit den Richtlinien für Zugriffsrechte anhängen und anschließend Benutzergruppe erstellen auswählen.

   Nachdem Sie die IAM-Benutzergruppe mit der SES-Berechtigungsrichtlinie erstellt haben, können Sie einen SMTP-Benutzer von seiner aktuellen Inline-Richtlinie zu dieser Gruppenrichtlinie migrieren, wie in den verbleibenden Schritten beschrieben.
10. Wählen Sie unter Zugriffsverwaltung die Option Benutzer und anschließend den SMTP-Benutzer aus, den Sie migrieren möchten.
11. Wählen Sie die Registerkarte Gruppen und dann Benutzer zu Gruppen hinzufügen aus.
12. Wählen Sie die `AWSSESSendingGroupDoNotRename` Gruppe aus, gefolgt von Benutzer zu Gruppe (n) hinzufügen.
13. Wählen Sie die Registerkarte Berechtigungen und vergewissern Sie sich, dass in `AmazonSesSendingAccess` der Spalte Richtlinienname zwei Zeilen mit dem aufgeführt sind, eine Zeile mit Inline und eine mit Gruppe *`AWSSESSendingGroupDoNotRename`* in der Spalte Angehangen über.
14. Wählen Sie nur die Zeile aus, die `AmazonSesSendingAccess` in der Spalte Richtlinienname und Inline in der Spalte Angehangen über enthält, gefolgt von Entfernen und bestätigen Sie mit Richtlinie entfernen.

    Vergewissern Sie sich, dass die Zeile mit Gruppe *`AWSSESSendingGroupDoNotRename`* in der Spalte Angefügt über erhalten bleibt.
15. Wählen Sie die Registerkarte „Tags“ und anschließend „Tags verwalten“.
16. Wählen Sie neben der Zeile, die in der Spalte Schlüssel und InvokedBySESConsolein der Spalte Wert enthält, Entfernen aus, gefolgt von Änderungen speichern.

> **Important**
>
> Die `AmazonSesSendingAccess` Richtlinie (entweder als Inline- oder Gruppenrichtlinie oder beides) muss dem SMTP-Benutzer zugeordnet bleiben, um sicherzustellen, dass dessen Versand nicht beeinträchtigt wird. Entfernen Sie die Inline-Richtlinie erst, nachdem die Gruppenrichtlinie Ihrem Benutzer zugewiesen wurde.

Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt

Um E-Mails über die Amazon SES SMTP-Schnittstelle zu senden, müssen Sie Ihre Anwendung mit einem SMTP-Endpunkt verbinden. Eine vollständige Liste der SMTP-Endpunkte von Amazon SES finden Sie unter Endpunkte und Kontingente von Amazon Simple Email Service in der Allgemeine AWS-Referenz.

Der SMTP-Endpunkt von Amazon SES erfordert, dass alle Verbindungen mit Transport Layer Security (TLS) verschlüsselt werden. (Beachten Sie, dass TLS häufig mit dem Namen des Vorgängerprotokolls, SSL, bezeichnet wird.) Amazon SES unterstützt zwei Mechanismen zum Einrichten einer TLS-verschlüsselten Verbindung: STARTTLS und TLS Wrapper. Lesen Sie in der Dokumentation für Ihre Software nach, um zu bestimmen, ob STARTTLS, TLS Wrapper oder beides unterstützt wird.

Amazon Elastic Compute Cloud (Amazon EC2) schränkt standardmäßig E-Mail-Verkehr über Port 25 ein. Um Zeitüberschreitungen beim Senden von E-Mails über den SMTP-Endpunkt von EC2 zu vermeiden, übermitteln Sie eine Anforderung zum Entfernen von E-Mail-Sendelimits, um die Drosselung zu entfernen. Alternativ können Sie E-Mails über einen anderen Port enden oder einen Amazon-VPC-Endpunkt verwenden.

Informationen zu SMTP-Verbindungsproblemen finden Sie unter SMTP-Probleme.

STARTTLS

STARTTLS ist ein Verfahren zum Upgraden einer unverschlüsselten Verbindung zu einer verschlüsselten Verbindung. Es stehen Versionen von STARTTLS für eine Reihe von Protokollen zur Verfügung. Die SMTP-Version ist in RFC 3207 definiert.

Zum Einrichten einer STARTTLS-Verbindung stellt der SMTP-Client eine Verbindung zum Amazon-SES-SMTP-Endpunkt auf Port 25, 587 oder 2587 her, gibt einen EHLO-Befehl aus und wartet, bis der Server mitgeteilt hat, dass er die STARTTLS-SMTP-Erweiterung unterstützt. Der Client gibt

dann den Befehl STARTTLS aus, um die TLS-Aushandlung zu initiieren. Wenn die Aushandlung abgeschlossen ist, gibt der Client über die neue verschlüsselte Verbindung einen EHLO-Befehl aus und die SMTP-Sitzung wird normal fortgesetzt.

TLS Wrapper

TLS Wrapper (auch bekannt als SMTPS oder Handshake Protocol) ist ein Verfahren zum Initiieren einer verschlüsselten Verbindung, ohne zuvor eine unverschlüsselte Verbindung herzustellen. Bei TLS Wrapper werden vom Amazon-SES-SMTP-Endpunkt keine TLS-Aushandlungen durchgeführt. Es liegt in der Verantwortung des Clients, eine Verbindung mit dem Endpunkt über TLS herzustellen und TLS dann für die gesamte Konversation weiterzuverwenden. TLS Wrapper ist ein älteres Protokoll, wird jedoch von vielen Clients weiterhin unterstützt.

Zum Einrichten einer TLS Wrapper-Verbindung stellt der SMTP-Client eine Verbindung mit dem Amazon-SES-SMTP-Endpunkt auf Port 465 oder 2465 her. Der Server repräsentiert sein Zertifikat, der Client gibt einen EHLO-Befehl aus und die SMTP-Sitzung wird normal fortgesetzt.

Senden von E-Mails über Amazon SES mithilfe von Softwarepaketen

Es gibt zahlreiche kommerzielle und Open Source-Softwarepakete, die das Senden von E-Mails über SMTP unterstützen. Hier sind einige Beispiele:

- Blog-Plattformen
- RSS-Aggregatoren
- Listenverwaltungssoftware
- Workflow-Systeme

Sie können alle diese SMTP-fähige Software für das Senden von E-Mails über die Amazon-SES-SMTP-Schnittstelle konfigurieren. Anweisungen zum Konfigurieren von SMTP für ein bestimmtes Softwarepaket finden Sie in der Dokumentation zu dieser Software.

Das folgende Verfahren zeigt, wie Sie Amazon-SES-Senden in JIRA einrichten, einer beliebten Problemverfolgungslösung. Mit dieser Konfiguration kann JIRA Benutzer per E-Mail benachrichtigen, wenn es eine Änderung am Status eines Softwareproblems gibt.

So konfigurieren Sie JIRA für das Senden von E-Mails mit Amazon SES

1. Melden Sie sich über einen Webbrowser mit Administrator-Anmeldeinformationen bei JIRA an.

2. Wählen Sie im Browserfenster Administration aus.
3. Wählen Sie im Menü System die Option Mail aus.
4. Wählen Sie auf der Seite Mail administration (Mail-Administration) die Option Mail Servers (Mail-Server) aus.
5. Klicken Sie auf Configure new SMTP mail server (Neuen SMPT-Mail-Server konfigurieren).
6. Füllen Sie im Formular Add SMTP Mail Server (SMPT-Mail-Server hinzufügen) die folgenden Felder aus:

   a. Name – Ein aussagekräftiger Name für diesen Server.

   b. Von Adresse – Die Adresse, von der die E-Mail gesendet wird. Sie müssen diese E-Mail-Adresse mit Amazon SES verifizieren, bevor Sie von ihr aus senden können. Weitere Informationen zur Verifizierung finden Sie unter Verifizierte Identitäten in Amazon SES.

   c. Email prefix – Eine Zeichenfolge, die JIRA vor dem Senden jeder Betreffzeile voranstellt.

   d. Protocol – Wählen Sie SMTP aus.

   > **Note**
   >
   > Wenn Sie keine Verbindung zu Amazon SES herstellen können, versuchen Sie SECURE_SMTP.

   e. Hostname – Eine Liste der Amazon-SES-SMTP-Endpunkte finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt. Wenn Sie beispielsweise den Amazon SES Endpunkt in der Region USA West (Oregon) verwenden möchten, lautet der Hostname email-smtp.us-west-2.amazonaws.com.

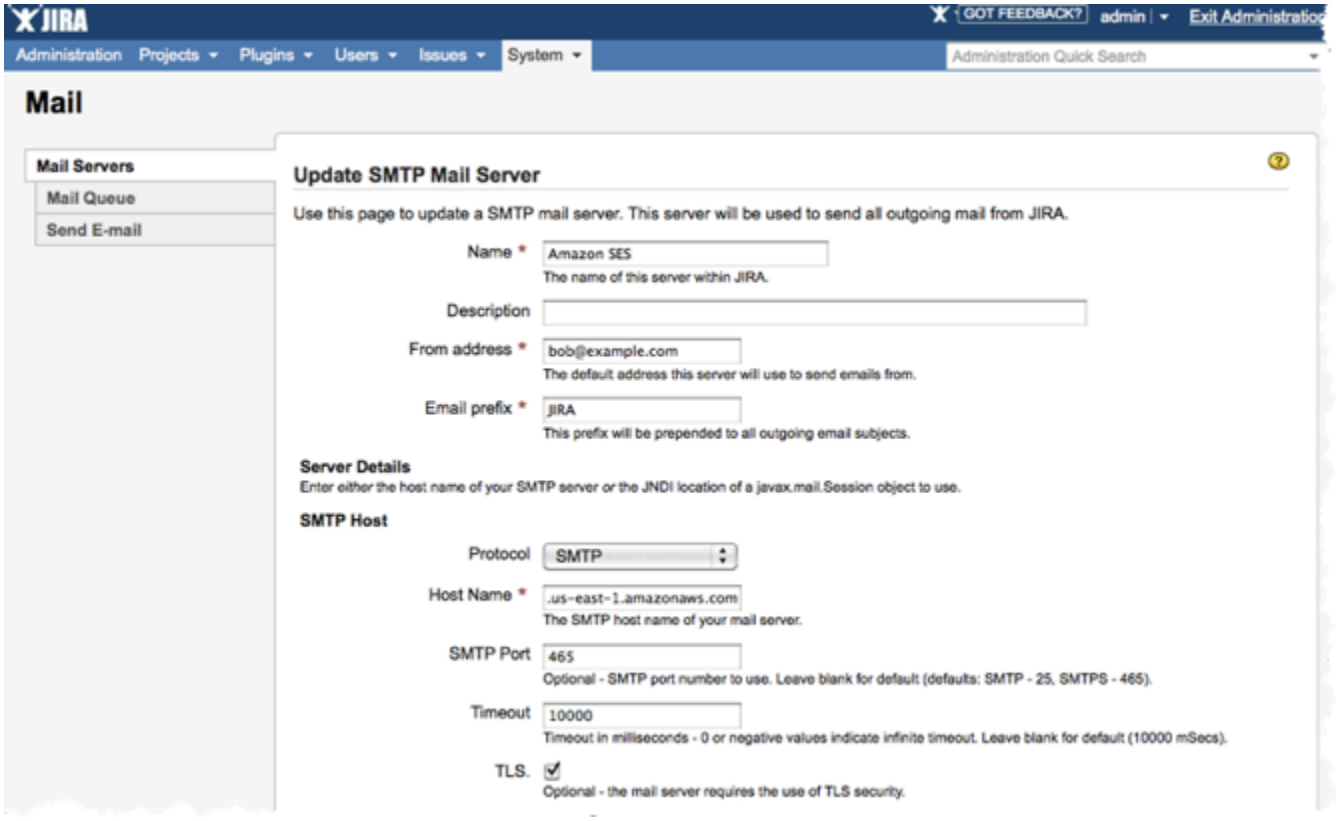
   f. SMTP-Port – 25, 587 oder 2587 (für eine Verbindung mit STARTTLS) oder 465 oder 2465 (für eine Verbindung mit TLS Wrapper).

   g. TLS – Aktivieren Sie dieses Kontrollkästchen.

   h. User name – Ihr -SMTP-Benutzername.

   i. Password – Ihr SMTP-Passwort.

   Die Einstellungen für TLS Wrapper finden Sie im folgenden Abbild.



7. Wählen Sie Test Connection (Verbindung testen) aus. Wenn die Test-E-Mail, die JIRA über Amazon SES sendet, eingeht, ist Ihre Konfiguration erfolgreich abgeschlossen.

Programmatisches Senden einer E-Mail über die Amazon-SES-SMTP-Schnittstelle

Um eine E-Mail über die Amazon-SES-SMTP-Schnittstelle zu versenden, können Sie eine SMTP-fähige Programmiersprache, einen Mailserver oder eine Anwendung verwenden. Bevor Sie beginnen, führen Sie die Aufgaben in Amazon Simple Email Service einrichten durch. Außerdem benötigen Sie die folgenden zusätzlichen Informationen:

- Ihre SMTP-Anmeldeinformationen für Amazon SES, mit denen Sie sich mit dem SMTP-Endpunkt von Amazon SES verbinden können. Informationen zum Abrufen Ihrer SMTP-Anmeldeinformationen für Amazon SES finden Sie unter Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen.

> **Important**
>
> Ihre SMTP-Anmeldeinformationen unterscheiden sich von Ihren AWS Anmeldeinformationen. Weitere Informationen zu Anmeldeinformationen finden Sie unter Arten von Amazon-SES-Anmeldeinformationen.

- Die SMTP-Endpunktadresse. Eine Liste der Amazon SES-SMTP-Endpunkte finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt.
- Die Port-Nummer der Amazon-SES-SMTP-Schnittstelle. Diese hängt von der Verbindungsmethode ab. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt.

Codebeispiele

Sie können auf die Amazon-SES-SMTP-Schnittstelle zugreifen, indem Sie eine SMTP-fähige Programmiersprache verwenden. Sie geben den Amazon-SES-SMTP-Hostnamen und die Port-Nummer zusammen mit Ihren SMTP-Anmeldeinformationen an und verwenden dann die generischen SMTP-Funktionen der Programmiersprache, um die E-Mail zu versenden.

Amazon Elastic Compute Cloud (Amazon EC2) schränkt standardmäßig den E-Mail-Datenverkehr über Port 25. Um Zeitüberschreitungen beim Senden von E-Mails über den SMTP-Endpunkt von Amazon EC2 zu vermeiden, können Sie beantragen, dass diese Einschränkungen entfernt werden. Weitere Informationen finden Sie unter Wie entferne ich die Beschränkung für Port 25 aus meiner Amazon EC2 EC2-Instance oder AWS Lambda -Funktion? im AWS Knowledge Center.

Die Codebeispiele in diesem Abschnitt für Java und PHP verwenden Port 587, um dieses Problem zu vermeiden.

> **Note**
>
> In diesem Tutorial senden Sie eine E-Mail an sich selbst, um zu prüfen, ob diese bei Ihnen ankommt. Für weitere Experimente oder Lasttests nutzen Sie den Amazon SES-Postfachsimulator. E-Mails, die Sie an den Postfachsimulator senden, zählen nicht zu Ihrer Sendequote oder Ihre Unzustellbarkeits- und Beschwerderate. Weitere Informationen finden Sie unter Manuelles Verwenden des Postfachsimulators.

Wählen Sie eine Programmiersprache aus, um das Beispiel für diese Sprache anzuzeigen:

> **Warning**
>
> Amazon SES empfiehlt nicht, statische Anmeldeinformationen zu verwenden. Unter erfahren AWS Secrets ManagerSie, wie Sie Ihre Sicherheitslage verbessern können, indem Sie hartcodierte Anmeldeinformationen aus Ihrem Quellcode entfernen. Dieses Tutorial dient nur dazu, die Amazon SES SMTP-Schnittstelle in einer Nicht-Produktionsumgebung zu testen.

Java

In diesem Beispiel werden die Eclipse-IDE und die JavaMail API verwendet, um E-Mails über Amazon SES mithilfe der SMTP-Schnittstelle zu senden.

Führen Sie erst die unter Amazon Simple Email Service einrichten beschriebenen Aufgaben aus, bevor Sie mit dem folgenden Verfahren beginnen.

So senden Sie eine E-Mail über die Amazon-SES-SMTP-Schnittstelle mit C#

1. Rufen Sie die JavaMail GitHub Seite in einem Webbrowser auf. Wählen Sie unter Assets die Option javax.mail.jar aus, um die neueste Version von herunterzuladen. JavaMail

   > **Important**
   >
   > Für dieses Tutorial ist Version 1.5 oder höher erforderlich JavaMail . Diese Verfahren wurden mit JavaMail Version 1.6.1 getestet.

2. Rufen Sie in einem Webbrowser die GitHub Jakarta-Aktivierungsseite auf und laden Sie unter JavaBeans Activation Framework 1.2.1 Final Release die Datei jakarta.activation.jar herunter
3. Erstellen Sie ein Projekt in Eclipse, indem Sie die folgenden Schritte ausführen:

   a. Starten Sie Eclipse.

   b. Wählen Sie in Eclipse die Optionen File (Datei), New (Neu) und dann Java Project (Java–Projekt) aus.

   c. Geben Sie im Dialogfeld Create a Java Project (Ein Java-Projekt erstellen) einen Projektnamen ein und klicken Sie auf Next (Weiter).

d. Wählen Sie im Dialogfeld Java Settings (Java-Einstellungen) die Registerkarte Libraries (Bibliotheken) aus.

e. Wählen Sie Classpath aus und fügen Sie die beiden externen JAR-Dateien javax.mail.jar und jakarta.activation.jar hinzu, indem Sie auf die Schaltfläche External hinzufügen klicken. JARs

f. Wählen Sie Extern JARs hinzufügen.

g. Navigieren Sie zu dem Ordner, in den Sie die Datei heruntergeladen haben JavaMail. Wählen Sie die Datei `javax.mail.jar` und dann Open (Öffnen) aus.

h. Klicken Sie im Dialogfeld Java Settings (Java-Einstellungen) auf Finish (Abschließen).

4. Erweitern Sie im Eclipse-Fenster Package Explorer (Paket-Explorer) das Projekt.

5. Klicken Sie unter Ihrem Projekt mit der rechten Maustaste auf das Verzeichnis src und wählen Sie New (Neu) und dann Class (Klasse) aus.

6. Geben Sie im Dialogfeld New Java Class (Neue Java-Klasse) im Feld Name die Zeichenfolge `AmazonSESSample` ein und klicken Sie auf Finish (Abschließen).

7. Ersetzen Sie den gesamten Inhalt von Amazon SESSample .java durch den folgenden Code:

```
import java.util.Properties;

import javax.mail.Message;
import javax.mail.Session;
import javax.mail.Transport;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;

public class AmazonSESSample {

    // Replace sender@example.com with your "From" address.
    // This address must be verified.
    static final String FROM = "sender@example.com";
    static final String FROMNAME = "Sender Name";

    // Replace recipient@example.com with a "To" address. If your account
    // is still in the sandbox, this address must be verified.
    static final String TO = "recipient@example.com";

    // Replace smtp_username with your Amazon SES SMTP user name.
    static final String SMTP_USERNAME = "smtp_username";
```

```
    // The name of the Configuration Set to use for this message.
    // If you comment out or remove this variable, you will also need to
    // comment out or remove the header below.
    static final String CONFIGSET = "ConfigSet";

    // Amazon SES SMTP host name. This example uses the US West (Oregon) region.
    // See https://docs.aws.amazon.com/ses/latest/DeveloperGuide/
regions.html#region-endpoints
    // for more information.
    static final String HOST = "email-smtp.us-west-2.amazonaws.com";

    // The port you will connect to on the Amazon SES SMTP endpoint.
    static final int PORT = 587;

    static final String SUBJECT = "Amazon SES test (SMTP interface accessed
 using Java)";

    static final String BODY = String.join(
            System.getProperty("line.separator"),
            "<h1>Amazon SES SMTP Email Test</h1>",
            "<p>This email was sent with Amazon SES using the ",
            "<a href='https://github.com/javaee/javamail'>Javamail Package</a>",
            " for <a href='https://www.java.com'>Java</a>."
        );

    public static void main(String[] args) throws Exception {

        // Create a Properties object to contain connection configuration
 information.
        Properties props = System.getProperties();
        props.put("mail.transport.protocol", "smtp");
        props.put("mail.smtp.port", PORT);
        props.put("mail.smtp.starttls.enable", "true");
        props.put("mail.smtp.auth", "true");

        // Create a Session object to represent a mail session with the
 specified properties.
        Session session = Session.getDefaultInstance(props);

        // Create a message with the specified information.
        MimeMessage msg = new MimeMessage(session);
        msg.setFrom(new InternetAddress(FROM,FROMNAME));
        msg.setRecipient(Message.RecipientType.TO, new InternetAddress(TO));
        msg.setSubject(SUBJECT);
```

```
        msg.setContent(BODY,"text/html");

        // Add a configuration set header. Comment or delete the
        // next line if you are not using a configuration set
        msg.setHeader("X-SES-CONFIGURATION-SET", CONFIGSET);

        // Create a transport.
        Transport transport = session.getTransport();

        // Get the password
        String SMTP_PASSWORD = fetchSMTPPasswordFromSecureStorage();

        // Send the message.
        try
        {
            System.out.println("Sending...");

            // Connect to Amazon SES using the SMTP username and password you
 specified above.
            transport.connect(HOST, SMTP_USERNAME, SMTP_PASSWORD);

            // Send the email.
            transport.sendMessage(msg, msg.getAllRecipients());
            System.out.println("Email sent!");
        }
        catch (Exception ex) {
            System.out.println("The email was not sent.");
            System.out.println("Error message: " + ex.getMessage());
        }
        finally
        {
            // Close and terminate the connection.
            transport.close();
        }
    }

    static String fetchSMTPPasswordFromSecureStorage() {
        /* IMPLEMENT THIS METHOD */
        // For example, you might fetch it from a secure location or AWS Secrets
 Manager: https://aws.amazon.com/secrets-manager/
    }
}
```

8. Ersetzen Sie in Amazon SESSample .java die folgenden E-Mail-Adressen durch Ihre eigenen Werte:

   > **Important**
   >
   > Bei den E-Mail-Adressen ist die Groß-/Kleinschreibung nicht relevant. Vergewissern Sie sich, dass die Adressen exakt mit denen übereinstimmen, die Sie verifiziert haben.

   - *sender@example.com*— Ersetzen Sie es durch Ihre „Von“ -E-Mail-Adresse. Sie müssen diese Adresse verifizieren, bevor Sie das Programm ausführen. Weitere Informationen finden Sie unter Verifizierte Identitäten in Amazon SES.
   - *recipient@example.com*— Ersetze es durch deine „An“ -E-Mail-Adresse. Wenn sich Ihr Konto noch in der Sandbox befindet, müssen Sie diese Adresse verifizieren, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).
9. Ersetzen Sie in Amazon SESSample .java Folgendes durch Ihre eigenen Werte:

   - *smtp_username*— Ersetzen Sie es durch Ihre SMTP-Benutzernamen-Anmeldedaten. Beachten Sie, dass der SMTP-Benutzername eine 20-stellige Zeichenfolge aus Buchstaben und Zahlen ist und kein wirklicher Name.
   - *smtp_password*— Implementieren `fetchSMTPPasswordFromSecureStorage`, um das Passwort abzurufen.
10. (Optional) Wenn Sie einen Amazon SES SMTP-Endpunkt in einem AWS-Region anderen als verwenden möchten*email-smtp.us-west-2.amazonaws.com*, ändern Sie den Wert der Variablen `HOST` auf den Endpunkt, den Sie verwenden möchten. Eine Liste der Regionen, in denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.
11. (Optional) Wenn Sie beim Senden dieser E-Mail einen Konfigurationssatz senden möchten, ändern Sie den Wert der Variable *ConfigSet* in den Namen des Konfigurationssatzes. Weitere Informationen zu Konfigurationssätzen finden Sie unter Verwenden von Amazon SES-Konfigurationssätzen im.
12. Speichern Sie Amazon SESSample .java.
13. Wählen Sie Project (Projekt) und dann Build Project (Projekt entwickeln) aus. (Falls diese Option deaktiviert ist, kann die automatische Erstellung aktiviert sein.)

14. Wählen Sie Run (Ausführen) und dann erneut Run (Ausführen) aus, um das Programm zu starten und die E-Mail zu senden.
15. Überprüfen Sie die Ausgabe. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole „E-Mail gesendet!“ Andernfalls wird eine Fehlermeldung angezeigt.
16. Melden Sie sich am E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

PHP

In diesem Beispiel wird die PHPMailer Klasse verwendet, um E-Mails über Amazon SES mithilfe der SMTP-Schnittstelle zu senden.

Bevor Sie das folgende Verfahren ausführen, müssen Sie den Vorgang in Amazon Simple Email Service einrichten abschließen. Zusätzlich zur Einrichtung von Amazon SES müssen Sie die folgenden Voraussetzungen für das Senden von E-Mails mit PHP erfüllen:

Voraussetzungen:

- PHP installieren — PHP ist unter http://php.net/downloads.php verfügbar. Fügen Sie nach der Installation von PHP Ihren Umgebungsvariablen den Pfad zu PHP hinzu, damit Sie PHP von jeder Eingabeaufforderung aus ausführen können.
- Installieren Sie den Composer-Abhängigkeitsmanager — Nachdem Sie den Composer-Abhängigkeitsmanager installiert haben, können Sie die PHPMailer Klasse und ihre Abhängigkeiten herunterladen und installieren. Folgen Sie den Installationsanweisungen unter https://getcomposer.org/download, um Composer zu installieren.
- PHPMailer Klasse installieren — Führen Sie nach der Installation von Composer den folgenden Befehl aus, um die Klasse zu installieren: PHPMailer

  ```
  path/to/composer require phpmailer/phpmailer
  ```

  Ersetzen Sie den Befehl im vorherigen Befehl *path/to/* durch den Pfad, in dem Sie Composer installiert haben.

So senden Sie eine E-Mail über die Amazon-SES-SMTP-Schnittstelle mit PHP

1. Erstellen Sie eine Datei mit dem Namen amazon-ses-smtp-sample.php. Öffnen Sie die Datei mit einem Texteditor und fügen Sie folgenden Code ein:

```
<?php

// Import PHPMailer classes into the global namespace
// These must be at the top of your script, not inside a function
use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\Exception;

// If necessary, modify the path in the require statement below to refer to the
// location of your Composer autoload.php file.
require 'vendor/autoload.php';

// Replace sender@example.com with your "From" address.
// This address must be verified with Amazon SES.
$sender = 'sender@example.com';
$senderName = 'Sender Name';

// Replace recipient@example.com with a "To" address. If your account
// is still in the sandbox, this address must be verified.
$recipient = 'recipient@example.com';

// Replace smtp_username with your Amazon SES SMTP user name.
$usernameSmtp = 'smtp_username';

// Specify a configuration set. If you do not want to use a configuration
// set, comment or remove the next line.
$configurationSet = 'ConfigSet';

// If you're using Amazon SES in a region other than US West (Oregon),
// replace email-smtp.us-west-2.amazonaws.com with the Amazon SES SMTP
// endpoint in the appropriate region.
$host = 'email-smtp.us-west-2.amazonaws.com';
$port = 587;

// The subject line of the email
$subject = 'Amazon SES test (SMTP interface accessed using PHP)';

// The plain-text body of the email
$bodyText =  "Email Test\r\nThis email was sent through the
    Amazon SES SMTP interface using the PHPMailer class.";

// The HTML-formatted body of the email
$bodyHtml = '<h1>Email Test</h1>
    <p>This email was sent through the
```

```
    <a href="https://aws.amazon.com/ses">Amazon SES</a> SMTP
    interface using the <a href="https://github.com/PHPMailer/PHPMailer">
    PHPMailer</a> class.</p>';

$mail = new PHPMailer(true);

try {
    // Specify the SMTP settings.
    $mail->isSMTP();
    $mail->setFrom($sender, $senderName);
    $mail->Username   = $usernameSmtp;
    $mail->Password   = fetchSMTPPasswordFromSecureStorage();
    $mail->Host       = $host;
    $mail->Port       = $port;
    $mail->SMTPAuth   = true;
    $mail->SMTPSecure = 'tls';
    $mail->addCustomHeader('X-SES-CONFIGURATION-SET', $configurationSet);

    // Specify the message recipients.
    $mail->addAddress($recipient);
    // You can also add CC, BCC, and additional To recipients here.

    // Specify the content of the message.
    $mail->isHTML(true);
    $mail->Subject    = $subject;
    $mail->Body       = $bodyHtml;
    $mail->AltBody    = $bodyText;
    $mail->Send();
    echo "Email sent!" , PHP_EOL;
} catch (phpmailerException $e) {
    echo "An error occurred. {$e->errorMessage()}", PHP_EOL; //Catch errors from
 PHPMailer.
} catch (Exception $e) {
    echo "Email not sent. {$mail->ErrorInfo}", PHP_EOL; //Catch errors from
 Amazon SES.
}
function fetchSMTPPasswordFromSecureStorage() {
/* IMPLEMENT THIS METHOD */
// For example, you might fetch it from a secure location or AWS Secrets
 Manager: https://aws.amazon.com/secrets-manager/
}

?>
```

2. Ersetzen Sie in amazon-ses-smtp-sample.php Folgendes durch Ihre eigenen Werte:

   - *sender@example.com*— Ersetzen Sie durch eine E-Mail-Adresse, die Sie bei Amazon SES verifiziert haben. Weitere Informationen finden Sie unter Verifizierte Identitäten. Bei den E-Mail-Adressen in Amazon SES wird die Groß-/Kleinschreibung beachtet. Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
   - *recipient@example.com*— Durch die Adresse des Empfängers ersetzen. Wenn sich Ihr Konto noch in der Sandbox befindet, müssen Sie diese Adresse verifizieren, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox). Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
   - *smtp_username*— Ersetzen Sie es durch Ihre SMTP-Benutzernamen-Anmeldedaten, die Sie auf der Seite mit den SMTP-Einstellungen der Amazon SES SES-Konsole abgerufen haben. Dieser Benutzername ist nicht mit Ihrer AWS -Zugriffsschlüssel-ID identisch. Beachten Sie, dass der SMTP-Benutzername eine 20-stellige Zeichenfolge aus Buchstaben und Zahlen ist und kein wirklicher Name.
   - *smtp_password*— Implementieren`fetchSMTPPasswordFromSecureStorage`, um das Passwort abzurufen.
   - (Optional) *ConfigSet* — Wenn Sie beim Senden dieser E-Mail einen Konfigurationssatz verwenden möchten, ersetzen Sie diesen Wert durch den Namen des Konfigurationssatzes. Weitere Informationen zu Konfigurationssätzen finden Sie unter Verwenden von Amazon SES-Konfigurationssätzen im.
   - (Optional) *email-smtp.us-west-2.amazonaws.com* — Wenn Sie einen Amazon SES SES-SMTP-Endpunkt in einer anderen Region als USA West (Oregon) verwenden möchten, ersetzen Sie diesen durch den Amazon SES SES-SMTP-Endpunkt in der Region, die Sie verwenden möchten. Eine Liste der SMTP-Endpunkte URLs , auf AWS-Regionen denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.
3. Speichern Sie die Datei amazon-ses-smtp-sample.php.
4. Um das Programm auszuführen, öffnen Sie eine Eingabeaufforderung im selben Verzeichnis wie amazon-ses-smtp-sample.php und geben Sie dann Folgendes ein. php amazon-ses-smtp-sample.php
5. Überprüfen Sie die Ausgabe. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole „E-Mail gesendet!“ an Andernfalls wird eine Fehlermeldung angezeigt.

6. Melden Sie sich am E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

Integrieren von Amazon SES in Ihren vorhandenen E-Mail-Server

Wenn Sie derzeit Ihren eigenen E-Mail-Server verwalten, können Sie den Amazon-SES-SMTP-Endpunkt zum Senden all Ihrer ausgehenden E-Mails an Amazon SES verwenden. Es ist nicht notwendig, die vorhandenen E-Mail-Clients und Anwendungen zu ändern. Die Umstellung auf Amazon SES ist transparent für diese.

Mehrere Mail Transfer Agents (MTAs) unterstützen das Senden von E-Mails über SMTP-Relays. Dieser Abschnitt enthält allgemeine Anleitungen zur Konfiguration einiger beliebter Apps für MTAs den E-Mail-Versand über die Amazon SES SMTP-Schnittstelle.

Der SMTP-Endpunkt von Amazon SES erfordert, dass alle Verbindungen mit Transport Layer Security (TLS) verschlüsselt werden.

Themen

- Integrieren von Amazon SES mit Postfix
- Integrieren von Amazon SES in Sendmail
- Integrieren von Amazon SES mit dem Microsoft Windows Server IIS SMTP

Integrieren von Amazon SES mit Postfix

Postfix ist eine Alternative zum weit verbreiteten Sendmail Message Transfer Agent (MTA). Weitere Informationen zu Postfix finden Sie unter http://www.postfix.org. Die Verfahren in diesem Thema funktionieren mit Linux, macOS, oder Unix.

> **Note**
>
> Postfix ist eine Drittanbieter-Anwendung und wird von Amazon Web Services nicht entwickelt oder unterstützt. Die Verfahren in diesem Abschnitt dienen ausschließlich zu Informationszwecken und können ohne vorherige Ankündigung geändert werden.

Voraussetzungen

Zum Abschließen der Verfahren in diesem Abschnitt müssen Sie zunächst folgende Aufgaben durchführen:

- Deinstallieren Sie die Sendmail-Anwendung, wenn sie bereits auf Ihrem System installiert ist. Das Verfahren für die Ausführung dieses Schritts variiert je nach verwendetem Betriebssystem.

  > **Important**
  >
  > Die folgenden Verweise auf sendmail beziehen sich auf den Postfix-Befehl `sendmail`, nicht zu verwechseln mit der Sendmail-Anwendung.

- Installieren Sie Postfix. Das Verfahren für die Ausführung dieses Schritts variiert je nach verwendetem Betriebssystem.
- Installieren Sie ein SASL-Authentifizierungspaket. Das Verfahren für die Ausführung dieses Schritts variiert je nach verwendetem Betriebssystem. Wenn Sie beispielsweise ein RedHat basiertes System verwenden, sollten Sie das `cyrus-sasl-plain` Paket installieren. Wenn Sie ein Debian- oder Ubuntu-basiertes System verwenden, sollten Sie das `libsasl2-modules`-Paket installieren.
- Überprüfen Sie eine E-Mail-Adresse oder Domäne, die für das Senden von E-Mails verwendet werden soll. Weitere Informationen finden Sie unter Erstellen einer E-Mail-Adressidentität.
- Wenn sich Ihr Konto noch in der Sandbox befindet, können Sie nur E-Mails an verifizierte E-Mail-Adressen senden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).

Konfigurieren von Postfix

Führen Sie die folgenden Verfahren durch, um Ihren E-Mail-Server für das Senden von E-Mail über Amazon SES mit Postfix zu konfigurieren.

So konfigurieren Sie Postfix

1. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
sudo postconf -e "relayhost = [email-smtp.us-west-2.amazonaws.com]:587" \
"smtp_sasl_auth_enable = yes" \
"smtp_sasl_security_options = noanonymous" \
"smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd" \
"smtp_use_tls = yes" \
```

```
"smtp_tls_security_level = secure" \
"smtp_tls_note_starttls_offer = yes"
```

> **Note**
>
> Wenn Sie Amazon SES in einer anderen AWS Region als USA West (Oregon) verwenden, ersetzen Sie *email-smtp.us-west-2.amazonaws.com* den vorherigen Befehl durch den SMTP-Endpunkt der entsprechenden Region. Weitere Informationen finden Sie unter the section called “Regionen”.

2. Öffnen Sie die Datei `/etc/postfix/master.cf` in einem Texteditor. Suchen Sie den folgenden Eintrag:

```
-o smtp_fallback_relay=
```

   Wenn Sie diesen Eintrag suchen, kommentieren Sie ihn aus, indem Sie ein # (Hash)-Zeichen an den Anfang der Zeile setzen. Speichern und schließen Sie die Datei.

   Wenn dieser Eintrag nicht vorhanden ist, fahren Sie mit dem nächsten Schritt fort.

3. Öffnen Sie die Datei `/etc/postfix/sasl_passwd` in einem Texteditor. Wenn die Datei nicht bereits vorhanden ist, erstellen Sie sie.

4. Fügen Sie die folgende Zeile zu `/etc/postfix/sasl_passwd` hinzu:

```
[email-smtp.us-west-2.amazonaws.com]:587 SMTPUSERNAME:SMTPPASSWORD
```

> **Note**
>
> Ersetzen Sie *SMTPUSERNAME* und *SMTPPASSWORD* durch Ihre SMTP-Anmeldeinformationen. Ihre SMTP-Anmeldeinformationen sind nicht mit Ihrer AWS -Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel identisch. Weitere Informationen zu Anmeldeinformationen finden Sie unter the section called “Abrufen Ihrer SMTP-Anmeldeinformationen”.
>
> Wenn Sie Amazon SES in einer anderen AWS Region als USA West (Oregon) verwenden, ersetzen Sie *email-smtp.us-west-2.amazonaws.com* das vorherige Beispiel durch den SMTP-Endpunkt der entsprechenden Region. Weitere Informationen finden Sie unter the section called “Regionen”.

Speichern und schließen Sie `sasl_passwd`.

5. Geben Sie bei der Eingabeaufforderung den folgenden Befehl ein, um eine Hashmap-Datenbankdatei mit Ihren SMTP-Anmeldeinformationen zu erstellen:

```
sudo postmap hash:/etc/postfix/sasl_passwd
```

6. (Optional) Die Dateien `/etc/postfix/sasl_passwd` und `/etc/postfix/sasl_passwd.db`, die Sie in den vorherigen Schritten erstellt haben, sind nicht verschlüsselt. Da diese Dateien Ihre SMTP-Anmeldeinformationen enthalten, empfehlen wir, dass Sie die Eigentümerschaft und Berechtigungen der Dateien ändern, um den Zugriff auf sie zu beschränken. So beschränken Sie den Zugriff auf diese Dateien:

   a. Geben Sie an einer Eingabeaufforderung den folgenden Befehl ein, um die Eigentümerschaft der Dateien zu ändern:

```
sudo chown root:root /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
```

   b. Geben Sie an einer Eingabeaufforderung den folgenden Befehl ein, um die Berechtigungen der Datei zu ändern, sodass nur der Root-Benutzer Lese- oder Schreiboperationen dafür ausführen kann:

```
sudo chmod 0600 /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
```

7. Teilen Sie Postfix mit, wo sich das CA-Zertifikat befindet (benötigt, um das Amazon-SES-Serverzertifikat zu überprüfen). Der Befehl in diesem Schritt variiert je nach Betriebssystem.

   - Wenn Sie Amazon Linux, Red Hat Enterprise Linux oder eine ähnliche Verteilung verwenden, geben Sie den folgenden Befehl ein:

```
sudo postconf -e 'smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt'
```

   - Wenn Sie Ubuntu oder eine ähnliche Verteilung verwenden, geben Sie den folgenden Befehl ein:

```
sudo postconf -e 'smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt'
```

- Wenn Sie macOS verwenden, können Sie das Zertifikat aus Ihrer System-Schlüsselkette generieren. Um das Zertifikat zu generieren, geben Sie den folgenden Befehl in der Befehlszeile ein:

  ```
  sudo security find-certificate -a -p /System/Library/Keychains/
  SystemRootCertificates.keychain | sudo tee /etc/ssl/certs/ca-bundle.crt > /dev/
  null
  ```

  Nachdem Sie den Zertifikattyp generiert haben, geben Sie den folgenden Befehl ein:

  ```
  sudo postconf -e 'smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt'
  ```

8. Geben Sie den folgenden Befehl ein, um den Postfix-Server zu starten (oder die Konfigurationseinstellungen neu zu laden, wenn der Server bereits ausgeführt wird):

   ```
   sudo postfix start; sudo postfix reload
   ```

9. Senden Sie eine Test-E-Mail, indem Sie den folgenden Befehl in die Befehlszeile eingeben und nach jeder Zeile die Eingabetaste drücken. Ersetzen Sie es *sender@example.com* durch Ihre Absender-E-Mail-Adresse. Die Absenderadresse muss für die Verwendung mit Amazon SES überprüft werden. *recipient@example.com*Durch die Zieladresse ersetzen. Wenn sich Ihr Konto noch in der Sandbox befindet, muss auch die Empfängeradresse verifiziert werden. Außerdem muss die letzte Zeile der Nachricht einen einzelnen Punkt (.) ohne andere Inhalte enthalten.

   ```
   sendmail -f sender@example.com recipient@example.com
   From: Sender Name <sender@example.com>
   Subject: Amazon SES Test
   This message was sent using Amazon SES.
   .
   ```

10. Überprüfen Sie das Postfach, das mit der Empfängeradresse verknüpft ist. Wenn die E-Mail nicht eintrifft, überprüfen Sie Ihren Spam-Ordner. Wenn Sie die E-Mail immer noch nicht finden können, überprüfen Sie das Mail-Protokoll auf dem System, das Sie zum Senden der E-Mail verwendet haben (in der Regel unter `/var/log/maillog` zu finden), um weitere Informationen zu erhalten.

Beispiel für die erweiterte Nutzung

In diesem Beispiel wird gezeigt, wie eine E-Mail versendet wird, die einen Konfigurationssatz verwendet und die eine MIME-Multipart-Codierung für das Senden sowohl eines Klartexts als auch einer HTML-Version der Nachricht mit einem Anhang nutzt. Sie beinhaltet auch einen Link-Tag, der für die Kategorisierung von Klickereignissen verwendet werden kann. Der Inhalt der E-Mail wird in einer externen Datei angegeben, sodass Sie die Befehle in der Postfix-Sitzung nicht manuell eingeben müssen.

So senden Sie eine mehrteilige MIME-E-Mail mit Postfix

1. Erstellen Sie in einem Texteditor eine neue Datei mit dem Namen `mime-email.txt`.
2. Fügen Sie in der Textdatei den folgenden Inhalt ein und ersetzen Sie dabei die roten Werte durch die entsprechenden Werte für Ihr Konto:

```
X-SES-CONFIGURATION-SET: ConfigSet
From:Sender Name <sender@example.com>
Subject:Amazon SES Test
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="YWVhZDFlY2QzMGQ2N2U0YTZmODU"

--YWVhZDFlY2QzMGQ2N2U0YTZmODU
Content-Type: multipart/alternative; boundary="3NjM0N2QwMTE4MWQ0ZTg2NTYxZQ"

--3NjM0N2QwMTE4MWQ0ZTg2NTYxZQ
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Amazon SES Test

This message was sent from Amazon SES using the SMTP interface.

For more information, see:
http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-smtp.html

--3NjM0N2QwMTE4MWQ0ZTg2NTYxZQ
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

<html>
  <head>
</head>
```

```
  <body>
    <h1>Amazon SES Test</h1>
      <p>This message was sent from Amazon SES using the SMTP interface.</p>
      <p>For more information, see
      <a ses:tags="samplekey0:samplevalue0;samplekey1:samplevalue1;"
      href="http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-
smtp.html">
      Using the Amazon SES SMTP Interface to Send Email</a> in the <em>Amazon SES
      Developer Guide</em>.</p>
  </body>
</html>
--3NjM0N2QwMTE4MWQ0ZTg2NTYxZQ--
--YWVhZDFlY2QzMGQ2N2U0YTZmODU
Content-Type: application/octet-stream
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="customers.txt"

SUQsRmlyc3ROYW1lLExhc3ROYW1lLENvdW50cnkKMzQ4LEpvaG4sU3RpbGVzLENh
bmFkYQo5MjM4OSxKaWUsTGl1LENoaW5hCjczNCxTaGlybGV5LFJvZHJpZ3VleixV
bml0ZWQgU3RhdGVzCjI4OTMsQW5heWEsSXllbmdhcixJbmRpYQ==
--YWVhZDFlY2QzMGQ2N2U0YTZmODU--
```

Speichern und schließen Sie die Datei.

3. Geben Sie in der Befehlszeile folgenden Befehl ein. *sender@example.com*Ersetzen Sie es durch Ihre E-Mail-Adresse und *recipient@example.com* ersetzen Sie es durch die E-Mail-Adresse des Empfängers.

   ```
   sendmail -f sender@example.com recipient@example.com < mime-email.txt
   ```

   Wenn der Befehl erfolgreich ausgeführt wird, wird er ohne Ausgabe beendet.

4. Suchen Sie in Ihrem Posteingang nach der E-Mail. Wenn die Nachricht nicht übermittelt wurde, überprüfen Sie das E-Mail-Protokoll Ihres Systems.

Integrieren von Amazon SES in Sendmail

Sendmail wurde in den frühen 80er-Jahren veröffentlicht und seitdem kontinuierlich verbessert. Es handelt sich dabei um einen flexiblen und konfigurierbaren Message Transfer Agent (MTA) mit einer großen Nutzer-Community. Sendmail wurde im Jahr 2013 von Proofpoint übernommen, Proofpoint bietet aber weiterhin eine Open-Source-Version von Sendmail an. Sie können die Open Source-

Version von Sendmail von der Proofpoint-Website oder über den Paket-Manager der meisten Linux-Distributionen herunterladen.

In Anleitung in diesem Abschnitt erfahren Sie, wie Sie Sendmail so konfigurieren, dass E-Mail-Nachrichten über Amazon SES gesendet werden. Dieses Verfahren wurde auf einem Server mit Ubuntu 18.04.2 LTS getestet.

> **Note**
>
> Sendmail ist eine Drittanbieter-Anwendung und wird von Amazon Web Services nicht entwickelt oder unterstützt. Die Verfahren in diesem Abschnitt dienen ausschließlich zu Informationszwecken und können ohne vorherige Ankündigung geändert werden.

Voraussetzungen

Bevor Sie das Verfahren in diesem Abschnitt ausführen, sollten Sie die folgenden Schritte ausführen:

- Installieren Sie das Sendmail-Paket auf Ihrem Server.

  > **Note**
  >
  > Je nachdem, welches Betriebssystem Sie verwenden, müssen Sie möglicherweise auch die folgenden Pakete installieren: `sendmail-cf`, `m4` und `cyrus-sasl-plain`.

- Überprüfen Sie die als „Von“-Adresse zu verwendende Identität. Weitere Informationen finden Sie unter Erstellen einer E-Mail-Adressidentität.

  Wenn Ihr Konto sich noch in der Amazon-SES-Sandbox befindet, müssen Sie auch die Adressen verifizieren, an die Sie E-Mail-Nachrichten senden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).

Wenn Sie Amazon SES benutzen, um E-Mail-Nachrichten von einer Amazon EC2-Instance aus zu senden, sollten Sie auch die folgenden Schritte ausführen:

- Sie müssen möglicherweise eine Elastic IP-Adresse zu Ihrer Amazon-EC2-Instance hinzufügen, damit empfangende E-Mail-Anbieter Ihre E-Mail-Nachrichten annehmen. Weitere Informationen finden Sie unter Amazon EC2 Elastic IP-Adressen im Amazon EC2 EC2-Benutzerhandbuch.

- Amazon Elastic Compute Cloud (Amazon EC2) schränkt den E-Mail-Datenverkehr standardmäßig über Port 25 ein. Um Zeitüberschreitungen beim Senden von E-Mails über den SMTP-Endpunkt von Amazon EC2 zu vermeiden, können Sie beantragen, dass diese Einschränkungen entfernt werden. Weitere Informationen finden Sie unter Wie entferne ich die Beschränkung für Port 25 aus meiner Amazon EC2 EC2-Instance oder AWS Lambda -Funktion? im AWS Knowledge Center.

  Alternativ können Sie das Verfahren in diesem Abschnitt ändern, um Port 587 anstelle von Port 25 zu verwenden.

Konfigurieren von Sendmail

Führen Sie die Schritte in diesem Abschnitt zum Konfigurieren von Sendmail für das Senden von E-Mail-Nachrichten mithilfe von Amazon SES aus.

> **Important**
>
> Bei dem Verfahren in diesem Abschnitt wird davon ausgegangen, dass Sie Amazon SES im Westen der USA (Oregon) verwenden möchten AWS-Region. Wenn Sie eine andere Region verwenden möchten, ersetzen Sie alle Instances von email-smtp.us-west-2.amazonaws.com in diesem Verfahren durch den SMTP-Endpunkt der gewünschten Region. Eine Liste der SMTP-Endpunkte URLs , auf AWS-Regionen denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.

So konfigurieren Sie Sendmail:

1. Öffnen Sie in einem Datei-Editor die Datei `/etc/mail/authinfo`. Wenn die Datei nicht vorhanden ist, erstellen Sie sie.

   Fügen Sie die folgende Zeile zu/etc/mail/authinfohinzu:

   ```
   AuthInfo:email-smtp.us-west-2.amazonaws.com "U:root" "I:smtpUsername"
    "P:smtpPassword" "M:PLAIN"
   ```

   Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

   - *email-smtp.us-west-2.amazonaws.com*Ersetzen Sie durch den Amazon SES SMTP-Endpunkt, den Sie verwenden möchten.
   - *smtpUsername*Ersetzen Sie es durch Ihren Amazon SES SMTP-Benutzernamen.

- *smtpPassword*Ersetzen Sie es durch Ihr Amazon SES SMTP-Passwort.

> **Note**
>
> Ihre SMTP-Anmeldedaten unterscheiden sich von Ihrer AWS Access Key-ID und Ihrem Secret Access Key. Weitere Informationen zum Abrufen Ihrer SMTP-Anmeldeinformationen finden Sie unter Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen.

Wenn Sie fertig sind, speichern Sie `authinfo`.

2. Geben Sie in der Befehlszeile den folgenden Befehl ein, um die `/etc/mail/authinfo.db`-Datei zu erstellen:

```
sudo sh -c 'makemap hash /etc/mail/authinfo.db < /etc/mail/authinfo'
```

3. Geben Sie in der Befehlszeile den folgenden Befehl ein, um die Unterstützung für die Weiterleitung an den Amazon-SES-SMTP-Endpunkt hinzuzufügen.

```
sudo sh -c 'echo "Connect:email-smtp.us-west-2.amazonaws.com RELAY" >> /etc/mail/
access'
```

Ersetzen Sie im vorherigen Befehl *email-smtp.us-west-2.amazonaws.com* durch die Adresse des Amazon SES SES-SMTP-Endpunkts, den Sie verwenden möchten.

4. Geben Sie in der Befehlszeile den folgenden Befehl ein, um/etc/mail/access.db neu zu generieren:

```
sudo sh -c 'makemap hash /etc/mail/access.db < /etc/mail/access'
```

5. Geben Sie in der Befehlszeile den folgenden Befehl ein, um Sicherungskopien der Dateien `sendmail.cf` und `sendmail.mc` zu erstellen:

```
sudo sh -c 'cp /etc/mail/sendmail.cf /etc/mail/sendmail_cf.backup && cp /etc/mail/
sendmail.mc /etc/mail/sendmail_mc.backup'
```

6. Fügen Sie der Datei/etc/mail/sendmail.mc vor allen Definitionen die folgenden Zeilen hinzu. `MAILER()`

```
define(`SMART_HOST', `email-smtp.us-west-2.amazonaws.com')dnl
define(`RELAY_MAILER_ARGS', `TCP $h 25')dnl
define(`confAUTH_MECHANISMS', `LOGIN PLAIN')dnl
FEATURE(`authinfo', `hash -o /etc/mail/authinfo.db')dnl
MASQUERADE_AS(`example.com')dnl
FEATURE(masquerade_envelope)dnl
FEATURE(masquerade_entire_domain)dnl
```

Gehen Sie im vorhergehenden Text wie folgt vor.

- *email-smtp.us-west-2.amazonaws.com*Ersetzen Sie durch den Amazon SES SMTP-Endpunkt, den Sie verwenden möchten.
- *example.com*Ersetzen Sie es durch die Domain, die Sie zum Senden von E-Mails verwenden möchten.

Wenn Sie fertig sind, speichern Sie die Datei.

> **Note**
>
> Amazon EC2 schränkt die Kommunikation standardmäßig über Port 25 ein. Wenn Sie Sendmail in einer Amazon-EC2-Instance verwenden, sollten Sie das Formular Anforderung zum Entfernen von E-Mail-Sendebeschränkungen ausfüllen.

7. Geben Sie in der Befehlszeile den folgenden Befehl ein, um sendmail.cf schreibfähig zu machen:

```
sudo chmod 666 /etc/mail/sendmail.cf
```

8. Geben Sie in der Befehlszeile den folgenden Befehl ein, um sendmail.cf erneut zu generieren:

```
sudo sh -c 'm4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf'
```

> **Note**
>
> Wenn Fehler, wie „Command not found (Befehl nicht gefunden“ und „No such file or directory (Verzeichnis nicht vorhanden)“ auftreten, stellen Sie sicher, dass die Pakete `m4` und `sendmail-cf` auf Ihrem System installiert sind.

9. Geben Sie in der Befehlszeile den folgenden Befehl ein, um die Berechtigungen von sendmail.cf auf „schreibgeschützt“ zurückzusetzen:

```
sudo chmod 644 /etc/mail/sendmail.cf
```

10. Geben Sie in der Befehlszeile den folgenden Befehl ein, um Sendmail neu zu starten:

```
sudo /etc/init.d/sendmail restart
```

Versuchen Sie je nach der Version von Linux oder Sendmail Folgendes, wenn das oben genannte nicht funktioniert:

```
sudo su service sendmail restart
```

11. Führen Sie die folgenden Schritte aus, um eine Test-E-Mail-Nachricht zu senden:

a. Geben Sie in der Befehlszeile den folgenden Befehl ein:

```
/usr/sbin/sendmail -vf sender@example.com recipient@example.com
```

*sender@example.com*Ersetzen Sie es durch Ihre Absender-E-Mail-Adresse. *recipient@example.com*Ersetzen Sie es durch die Empfängeradresse. Wenn Sie fertig sind, betätigen Sie Enter.

b. Geben Sie den folgenden Nachrichteninhalt ein. Betätigen Sie nach jeder Zeile Enter.

```
From: sender@example.com
To: recipient@example.com
Subject: Amazon SES test email

This is a test message sent from Amazon SES using Sendmail.
```

Wenn Sie den Inhalt der E-Mail-Nachricht eingegeben haben, betätigen Sie Ctrl+D, um sie zu senden.

12. Überprüfen Sie den E-Mail-Client des Empfängers auf die E-Mail-Nachricht. Wenn Sie die E-Mail-Nachricht nicht finden können, überprüfen Sie den Spam-Ordner. Wenn Sie die E-Mail-Nachricht immer noch nicht finden können, überprüfen Sie das Sendmail-Protokoll auf Ihrem E-Mail-Server. Das Protokoll befindet sich häufig unter/var/log/mail.log oder/var/log/maillog.

Integrieren von Amazon SES mit dem Microsoft Windows Server IIS SMTP

Sie können den IIS-SMTP-Server von Microsoft Windows für das Senden von E-Mails über Amazon SES konfigurieren. Diese Anweisungen wurden mit Microsoft Windows Server 2022 auf einer Amazon EC2 EC2-Instance geschrieben. Sie können dieselbe Konfiguration auf Microsoft Windows Server 2016 verwenden.

> **Note**
>
> Windows Server ist eine Drittanbieteranwendung und wird von Amazon Web Services nicht entwickelt oder unterstützt. Die Verfahren in diesem Abschnitt dienen ausschließlich zu Informationszwecken und können ohne vorherige Ankündigung geändert werden.

So integrieren Sie den IIS-SMTP-Server von Microsoft Windows in Amazon SES

1. Richten Sie zunächst Microsoft Windows Server 2022 mithilfe der folgenden Anweisungen ein.
    a. Starten Sie von der Amazon EC2-Managementkonsole aus eine neue Amazon EC2 EC2-Basisinstanz für Microsoft Windows Server 2022.
    b. Stellen Sie eine Verbindung mit der Instance über Remote Desktop her und melden Sie sich an. Befolgen Sie hierzu die Anweisungen unter Erste Schritte mit Amazon EC2 Windows-Instances.
    c. Starten Sie das Server Manager-Dashboard.
    d. Installieren Sie die Rolle Web Server. Stellen Sie sicher, dass Sie die IIS 10-Verwaltungskompatibilitätstools (eine Option unter dem Kontrollkästchen Webserver) einbeziehen.
    e. Installieren Sie die Funktion SMTP Server.
2. Anschließend konfigurieren Sie den IIS-SMTP-Service unter Verwendung der folgenden Anweisungen.
    a. Kehren Sie zum Server-Manager-Dashboard zurück.
    b. Wählen Sie im Menü Tools die Option Internet Information Services (IIS) 10.0 Manager aus.
    c. Klicken Sie mit der rechten Maustaste auf SMTP Virtual Server #1 und wählen Sie anschließend Properties (Eigenschaften) aus.
    d. Wählen Sie auf der Registerkarte Access (Zugreifen) unter Relay Restrictions (Relais-Einschränkungen) die Option Relay (Relais) aus.

e. Klicken Sie im Dialogfeld Relay Restrictions (Relais-Einschränkungen auf Add (Hinzufügen).

f. Geben Sie unter Single Computer 127.0.0.1 für die IP-Adresse ein. Sie haben diesem Server nun Zugriff gewährt, um E-Mails über den IIS-SMTP-Service an Amazon SES weiterzuleiten.

   In diesem Verfahren gehen wir davon aus, dass Ihre E-Mails auf diesem Server generiert werden. Wenn die Anwendung, die die E-Mails generiert, auf einem separaten Server ausgeführt wird, müssen Sie Weiterleitungszugriff für diesen Server in IIS-SMTP gewähren.

> **Note**
>
> Um die SMTP-Weiterleitung auf private Subnetze zu erweitern, wählen Sie für Relay Restriction (Relais-Einschränkungen) Single Computer (Einzelcomputer) 127.0.0.1 und Group of Computers (Gruppe von Computern) 172.1.1.0 - 255.255.255.0 (im Bereich mit der Netzwerkmaske). Verwenden Sie für Connection (Verbindung) Single Computer (Einzelcomputer) 127.0.0.1 und Group of Computers (Gruppe von Computern) 172.1.1.0 - 255.255.255.0 (im Bereich mit der Netzwerkmaske).

3. Konfigurieren Sie schließlich den Server für das Senden von E-Mails über Amazon SES mithilfe der folgenden Anweisungen.

   a. Kehren Sie zum Dialogfeld SMTP Virtual Server #1 Properties zurück und wählen Sie die Register Delivery (Bereitstellung) aus.

   b. Wählen Sie auf der Registerkarte Delivery (Bereitstellung) die Option Outbound Security (Ausgehende Sicherheit) aus.

   c. Wählen Sie Basic Authentication (Standardauthentifizierung) aus und geben Sie dann Ihre SMTP-Anmeldeinformationen für Amazon SES ein. Sie können diese Anmeldeinformationen aus der Amazon-SES-Konsole mit dem Verfahren unter Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen abrufen.

> **Important**
>
> Ihre SMTP-Anmeldeinformationen stimmen nicht mit Ihrer AWS Zugriffsschlüssel-ID und Ihrem geheimen Zugriffsschlüssel überein. Versuchen Sie nicht, sich mit Ihren AWS Anmeldeinformationen am SMTP-Endpunkt zu authentifizieren. Weitere

Informationen zu Anmeldeinformationen finden Sie unter Arten von Amazon-SES-Anmeldeinformationen.

d. Stellen Sie sicher, dass TLS encryption (TLS-Verschlüsselung) ausgewählt ist.
e. Kehren Sie zur Registerkarte Delivery (Bereitstellung) zurück.
f. Wählen Sie Outbound Connections (Ausgehende Verbindungen) aus.
g. Stellen Sie im Dialogfeld Outbound Connections (Ausgehende Verbindungen) sicher, dass der Port 25 oder 587 ist.
h. Wählen Sie Advanced (Erweitert) aus.
i. Geben Sie für den Smarthostnamen den Amazon SES Endpunkt ein, den Sie verwenden werden (zum Beispielemail-smtp.us-west-2.amazonaws.com). Eine Liste der Endpunkte, URLs auf AWS-Regionen denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.
j. Kehren Sie zum Server-Manager-Dashboard zurück.
k. Klicken Sie auf dem Server Manager-Dashboard mit der rechten Maustaste auf SMTP Virtual Server #1 und starten Sie dann den Service neu, damit die neue Konfiguration wirksam wird.
l. Senden Sie eine E-Mail über diesen Server. Sie können die Nachrichten-Header prüfen, um zu bestätigen, dass sie über Amazon SES zugestellt wurde.

Testen der Verbindung zur Amazon-SES-SMTP-Schnittstelle über die Befehlszeile

Die in diesem Abschnitt beschriebenen Methoden dienen dazu, Ihre Verbindung zum Amazon-SES-SMTP-Endpunkt zu testen, Ihre SMTP-Anmeldeinformationen zu überprüfen und Verbindungsprobleme zu beheben. Diese Verfahren verwenden Tools und Bibliotheken, die in den gängigsten Betriebssystemen enthalten sind.

Zusätzliche Hinweise zur Behebung von SMTP-Verbindungsproblemen finden Sie unter SMTP-Probleme bei Amazon SES.

Voraussetzungen

Wenn Sie eine Verbindung mit der Amazon-SES-SMTP-Schnittstelle herstellen, müssen Sie einen Satz von SMTP-Anmeldeinformationen angeben. Diese SMTP-Anmeldeinformationen unterscheiden sich von Ihren AWS Standardanmeldedaten. Die beiden Arten von Anmeldeinformationen sind nicht

austauschbar. Weitere Informationen zum Abrufen Ihrer SMTP-Anmeldeinformationen finden Sie unter the section called “Abrufen Ihrer SMTP-Anmeldeinformationen”.

Testen Ihrer Amazon SES SMTP-Schnittstellenverbindung

Sie können die Befehlszeile verwenden, um Ihre Verbindung zur Amazon-SES-SMTP-Schnittstelle zu testen, ohne sich zu authentifizieren oder Nachrichten zu senden. Dieses Verfahren ist nützlich für die Behebung grundlegender Verbindungsprobleme. Falls Ihre Testverbindung fehlschlägt, finden Sie weitere Informationen unter SMTP-Probleme.

Dieser Abschnitt enthält Verfahren zum Testen Ihrer Verbindung sowohl mit OpenSSL (das in den meisten Linux-, macOS- und Unix-Distributionen enthalten ist und auch für Windows verfügbar ist) als auch mit dem `Test-NetConnection` Cmdlet in PowerShell (das in den neuesten Versionen von Windows enthalten ist).

Linux, macOS, or Unix

Es gibt zwei Möglichkeiten, mit OpenSSL eine Verbindung zur Amazon-SES-SMTP-Schnittstelle herzustellen: mithilfe von explizitem SSL über Port 587 oder mithilfe von implizitem SSL über Port 465.

So stellen Sie eine Verbindung mit der SMTP-Schnittstelle über explizites SSL her:

- Geben Sie an der Befehlszeile den folgenden Befehl ein, um eine Verbindung mit dem Amazon SES-SMTP-Server herzustellen:

```
openssl s_client -crlf -quiet -starttls smtp -connect email-smtp.us-
west-2.amazonaws.com:587
```

Ersetzen Sie im vorherigen Befehl *email-smtp.us-west-2.amazonaws.com* durch die URL des Amazon SES SES-SMTP-Endpunkts für Ihre AWS Region. Weitere Informationen finden Sie unter the section called “Regionen”.

Wenn die Verbindung erfolgreich hergestellt wurde, sehen Sie in etwa die folgende Ausgabe:

```
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = email-smtp.us-west-2.amazonaws.com
```

```
verify return:1
250 Ok
```

Die Verbindung wird nach ca. 10 Sekunden Inaktivität automatisch geschlossen.

Alternativ können Sie implizites SSL verwenden, um über Port 465 eine Verbindung mit der SMTP-Schnittstelle herzustellen.

So stellen Sie eine Verbindung mit der SMTP-Schnittstelle über implizites SSL her:

- Geben Sie an der Befehlszeile den folgenden Befehl ein, um eine Verbindung mit dem Amazon SES-SMTP-Server herzustellen:

  ```
  openssl s_client -crlf -quiet -connect email-smtp.us-west-2.amazonaws.com:465
  ```

  Ersetzen Sie im vorherigen Befehl *email-smtp.us-west-2.amazonaws.com* durch die URL des Amazon SES SES-SMTP-Endpunkts für Ihre AWS Region. Weitere Informationen finden Sie unter the section called “Regionen”.

  Wenn die Verbindung erfolgreich hergestellt wurde, sehen Sie in etwa die folgende Ausgabe:

  ```
  depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
  verify return:1
  depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
  verify return:1
  depth=0 CN = email-smtp.us-west-2.amazonaws.com
  verify return:1
  220 email-smtp.amazonaws.com ESMTP SimpleEmailService-d-VCSHDP1YZ
   A1b2C3d4E5f6G7h8I9j0
  ```

  Die Verbindung wird nach ca. 10 Sekunden Inaktivität automatisch geschlossen.

PowerShell

Sie können das NetConnectionTest-Cmdlet in verwenden, PowerShell um eine Verbindung zum Amazon SES SMTP-Server herzustellen.

> **Note**
>
> Das `Test-NetConnection`-Cmdlet kann bestimmen, ob der Computer eine Verbindung zum Amazon-SES-SMTP-Endpunkt herstellen kann. Es wird jedoch nicht getestet, ob Ihr Computer eine implizite oder explizite SSL-Verbindung zum SMTP-Endpunkt herstellen kann. Um eine SSL-Verbindung zu testen, können Sie entweder OpenSSL für Windows installieren oder eine Test-E-Mail-Nachricht senden.

So stellen Sie eine Verbindung mit der SMTP-Schnittstelle über das **`Test-NetConnection`**-Cmdlet her:

- Geben Sie PowerShell unter den folgenden Befehl ein, um eine Verbindung zum Amazon SES SMTP-Server herzustellen:

  ```
  Test-NetConnection -Port 587 -ComputerName email-smtp.us-west-2.amazonaws.com
  ```

  Ersetzen Sie im vorherigen Befehl *`email-smtp.us-west-2.amazonaws.com`* durch die URL des Amazon SES SES-SMTP-Endpunkts für Ihre AWS Region und *`587`* ersetzen Sie ihn durch die Portnummer. Für weitere Informationen zu regionsspezifischen Endpunkten für Amazon SES sehen Sie the section called “Regionen”.

  Wenn die Verbindung erfolgreich war, sehen Sie eine Ausgabe, die dem folgenden Beispiel ähnelt:

  ```
  ComputerName     : email-smtp.us-west-2.amazonaws.com
  RemoteAddress    : 198.51.100.126
  RemotePort       : 587
  InterfaceAlias   : Ethernet
  SourceAddress    : 203.0.113.46
  TcpTestSucceeded : True
  ```

Verwenden der Befehlszeile zum Senden von E-Mails mithilfe der Amazon-SES-SMTP-Schnittstelle

Sie können auch die Befehlszeile verwenden, um Nachrichten mithilfe der Amazon-SES-SMTP-Schnittstelle zu senden. Dieses Verfahren ist nützlich, um SMTP-Anmeldeinformationen zu testen

und zu überprüfen, ob bestimmte Empfänger Nachrichten empfangen können, die Sie mithilfe von Amazon SES senden.

Linux, macOS, or Unix

Wenn ein E-Mail-Absender eine Verbindung zu einem SMTP-Server herstellt, gibt der Client einen Standardsatz von Anfragen aus und der Server beantwortet jede Anfrage mit einer Standardantwort. Diese Reihe von Anfragen und Antworten wird als eine SMTP-Aushandlung bezeichnet. Wenn Sie eine Verbindung mit dem Amazon SES SMTP-Server mithilfe von OpenSSL aufbauen, erwartet der Server eine SMTP-Aushandlung.

Wenn Sie OpenSSL verwenden, um eine Verbindung mit der SMTP-Schnittstelle herzustellen, müssen Sie Ihre SMTP-Anmeldeinformationen mit base64-Kodierung kodieren. Dieser Abschnitt enthält Verfahren zum Kodieren Ihrer Anmeldeinformationen mit base64.

So senden Sie eine E-Mail über die Befehlszeile mittels der SMTP-Schnittstelle

1. Geben Sie in der Befehlszeile Folgendes ein und *email-smtp.us-west-2.amazonaws.com* ersetzen Sie es durch die URL des Amazon SES SMTP-Endpunkts für Ihren AWS-Region. Weitere Informationen finden Sie unterthe section called “Regionen”. :

```
#!/bin/bash

# Prompt user to provide following information
read -p "Configuration set: " CONFIGSET
read -p "Enter SMTP username: " SMTPUsername
read -p "Enter SMTP password: " SMTPPassword
read -p "Sender email address: " MAILFROM
read -p "Receiver email address: " RCPT
read -p "Email subject: " SUBJECT
read -p "Message to send: " DATA

echo

# Encode SMTP username and password using base64
EncodedSMTPUsername=$(echo -n "$SMTPUsername" | openssl enc -base64)
EncodedSMTPPassword=$(echo -n "$SMTPPassword" | openssl enc -base64)

# Construct the email
Email="EHLO example.com
AUTH LOGIN
```

```
$EncodedSMTPUsername
$EncodedSMTPPassword
MAIL FROM: $MAILFROM
RCPT TO: $RCPT
DATA
X-SES-CONFIGURATION-SET: $CONFIGSET
From: $MAILFROM
To: $RCPT
Subject: $SUBJECT

$DATA
.
QUIT"

echo "$Email" | openssl s_client -crlf -quiet -starttls smtp -connect email-
smtp.us-west-2.amazonaws.com:587
```

2. Geben Sie an der Eingabeaufforderung für jede Variable Ihre Werte ein.
3. • Um mit implizitem SSL über Port 465 zu senden, verwenden Sie:

```
openssl s_client -crlf -quiet -connect email-smtp.us-west-2.amazonaws.com:465
```

Wenn die Nachricht von Amazon SES akzeptiert wurde, sehen Sie eine Ausgabe ähnlich dem folgenden Beispiel:

```
250 Ok 01010160d7de98d8-21e57d9a-JZho-416c-bbe1-8ebaAexample-000000
```

Die sich an `250 Ok` anschließende Abfolge von Zahlen und Text, ist die Nachrichten-ID der E-Mail.

> **Note**
>
> Die Verbindung wird nach ca. 10 Sekunden Inaktivität automatisch geschlossen.

PowerShell

Sie können Net.Mail verwenden. SmtpClientKlasse zum Senden von E-Mails mit explizitem SSL über Port 587.

> **Note**
>
> Die `Net.Mail.SmtpClient`-Klasse ist offiziell veraltet, und Microsoft empfiehlt, dass Sie Bibliotheken von Drittanbietern verwenden. Dieser Code ist nur für Testzwecke gedacht und sollte nicht für Produktionsarbeitslasten verwendet werden.

Um eine E-Mail PowerShell mit explizitem SSL zu senden

1. Erstellen Sie in einem Texteditor eine neue Datei. Fügen Sie folgenden Code in die Datei ein:

```
function SendEmail($Server, $Port, $Sender, $Recipient, $Subject, $Body) {
    $Credentials = [Net.NetworkCredential](Get-Credential)

    $SMTPClient = New-Object Net.Mail.SmtpClient($Server, $Port)
    $SMTPClient.EnableSsl = $true
    $SMTPClient.Credentials = New-Object
 System.Net.NetworkCredential($Credentials.Username, $Credentials.Password);

    try {
        Write-Output "Sending message..."
        $SMTPClient.Send($Sender, $Recipient, $Subject, $Body)
        Write-Output "Message successfully sent to $($Recipient)"
    } catch [System.Exception] {
        Write-Output "An error occurred:"
        Write-Error $_
    }
}

function SendTestEmail(){
    $Server = "email-smtp.us-west-2.amazonaws.com"
    $Port = 587

    $Subject = "Test email sent from Amazon SES"
    $Body = "This message was sent from Amazon SES using PowerShell (explicit
 SSL, port 587)."

    $Sender = "sender@example.com"
    $Recipient = "recipient@example.com"

    SendEmail $Server $Port $Sender $Recipient $Subject $Body
}
```

```
SendTestEmail
```

Wenn Sie fertig sind, speichern Sie die Datei unter `SendEmail.ps1`.

2. Nehmen Sie die folgenden Änderungen an der im vorherigen Schritt erstellten Datei vor:

   - *`sender@example.com`*Ersetzen Sie es durch die E-Mail-Adresse, von der Sie die Nachricht senden möchten.
   - *`recipient@example.com`*Ersetzen Sie es durch die E-Mail-Adresse, an die Sie die Nachricht senden möchten.
   - *`email-smtp.us-west-2.amazonaws.com`*Ersetzen Sie durch die URL des Amazon SES SMTP-Endpunkts für Ihre AWS Region. Weitere Informationen finden Sie unter Regionen und Amazon SES.

3. Geben Sie in PowerShell den folgenden Befehl ein:

   ```
   .\path\to\SendEmail.ps1
   ```

   Ersetzen Sie es im vorherigen Befehl *`path\to\SendEmail.ps1`* durch den Pfad zu der Datei, die Sie in Schritt 1 erstellt haben.

4. Wenn Sie dazu aufgefordert werden, geben Sie Ihren SMTP-Benutzernamen und Ihr Passwort ein.

Alternativ können Sie das System.Web.Mail verwenden. SmtpMailKlasse zum Senden von E-Mails mit implizitem SSL über Port 465.

> **Note**
>
> Die `System.Web.Mail.SmtpMail`-Klasse ist offiziell veraltet, und Microsoft empfiehlt, dass Sie Bibliotheken von Drittanbietern verwenden. Dieser Code ist nur für Testzwecke gedacht und sollte nicht für Produktionsarbeitslasten verwendet werden.

Um eine E-Mail PowerShell mit implizitem SSL zu senden

1. Erstellen Sie in einem Texteditor eine neue Datei. Fügen Sie folgenden Code in die Datei ein:

   ```
   [System.Reflection.Assembly]::LoadWithPartialName("System.Web") > $null
   ```

```
function SendEmail($Server, $Port, $Sender, $Recipient, $Subject, $Body) {
    $Credentials = [Net.NetworkCredential](Get-Credential)

    $mail = New-Object System.Web.Mail.MailMessage
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpserver", $Server)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpserverport", $Port)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpusessl", $true)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
sendusername", $Credentials.UserName)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
sendpassword", $Credentials.Password)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpconnectiontimeout", $timeout / 1000)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/sendusing",
 2)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpauthenticate", 1)

    $mail.From = $Sender
    $mail.To = $Recipient
    $mail.Subject = $Subject
    $mail.Body = $Body

    try {
        Write-Output "Sending message..."
        [System.Web.Mail.SmtpMail]::Send($mail)
        Write-Output "Message successfully sent to $($Recipient)"
    } catch [System.Exception] {
        Write-Output "An error occurred:"
        Write-Error $_
    }
}

function SendTestEmail(){
    $Server = "email-smtp.us-west-2.amazonaws.com"
    $Port = 465

    $Subject = "Test email sent from Amazon SES"
    $Body = "This message was sent from Amazon SES using PowerShell (implicit
 SSL, port 465)."
```

```
    $Sender = "sender@example.com"
    $Recipient = "recipient@example.com"

    SendEmail $Server $Port $Sender $Recipient $Subject $Body
}

SendTestEmail
```

Wenn Sie fertig sind, speichern Sie die Datei unter `SendEmail.ps1`.

2. Nehmen Sie die folgenden Änderungen an der im vorherigen Schritt erstellten Datei vor:

   - *sender@example.com*Ersetzen Sie es durch die E-Mail-Adresse, von der Sie die Nachricht senden möchten.
   - *recipient@example.com*Ersetzen Sie es durch die E-Mail-Adresse, an die Sie die Nachricht senden möchten.
   - *email-smtp.us-west-2.amazonaws.com*Ersetzen Sie durch die URL des Amazon SES SMTP-Endpunkts für Ihre AWS Region. Weitere Informationen finden Sie unter Regionen und Amazon SES.

3. Geben Sie in PowerShell den folgenden Befehl ein:

   ```
   .\path\to\SendEmail.ps1
   ```

   Ersetzen Sie es im vorherigen Befehl *path\to\SendEmail.ps1* durch den Pfad zu der Datei, die Sie in Schritt 1 erstellt haben.

4. Wenn Sie dazu aufgefordert werden, geben Sie Ihren SMTP-Benutzernamen und Ihr Passwort ein.

Verwenden der Amazon-SES-API zum Senden von E-Mails

Sie können die Simple Mail Transfer Protocol(SMTP)-Schnittstelle oder die Amazon SES-API verwenden, um Produktions-E-Mails über Amazon SES zu senden. Weitere Informationen über die SMTP-Schnittstelle finden Sie unter Verwenden der Amazon-SES-SMTP-Schnittstelle zum Senden von E-Mails. In diesem Abschnitt wird beschrieben, wie Sie mithilfe der API E-Mails senden.

Wenn Sie eine E-Mail über die API senden, geben Sie den Inhalt der Nachricht an, und Amazon SES stellt eine MIME-E-Mail für Sie zusammen. Alternativ können Sie die E-Mail selbst zusammenstellen,

sodass Sie die vollständige Kontrolle über den Inhalt der Nachricht haben. Weitere Informationen zur API finden Sie in der Amazon-Simple-Email-Service-API-Referenz. Eine Liste der Endpunkte URLs , auf AWS-Regionen denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service-Endpunkte und Kontingente in der Allgemeine AWS-Referenz.

Sie können die API wie folgt aufrufen:

- Stellen Sie direkte HTTPS-Anfragen -Dies ist die fortschrittlichste Methode, da Sie die Authentifizierung und Signieren Ihrer Anfragen manuell bearbeiten und die Anforderungen dann manuell erstellen müssen. Weitere Informationen zur Amazon SES API finden Sie unter derWillkommen-Seite in derAPI-v2-Referenzaus.
- Verwenden Sie ein AWS SDK —AWS SDKs erleichtern Sie den Zugriff APIs auf verschiedene AWS Dienste, einschließlich Amazon SES. Wenn Sie ein SDK verwenden, übernimmt es das Signieren der Anfragen, Authentifizierung, Wiederholungslogik, Fehlerbehandlung und andere Low-Level-Funktionen, damit Sie sich darauf konzentrieren können, Anwendungen zu entwickeln, die Ihre Kunden begeistern.
- Verwenden einer Befehlszeilenschnittstelle – Die AWS Command Line Interface ist das Befehlszeilentool für Amazon SES. Wir bieten die AWS Tools auch PowerShell für diejenigen an, die in der PowerShell Umgebung Skripte schreiben.

Unabhängig davon, ob Sie direkt oder indirekt über ein AWS SDK, die oder die AWS Tools für auf die AWS Command Line Interface Amazon SES SES-API zugreifen PowerShell, bietet Ihnen die Amazon SES SES-API zwei verschiedene Möglichkeiten, eine E-Mail zu senden, je nachdem, wie viel Kontrolle Sie über die Zusammensetzung der E-Mail-Nachricht haben möchten:

- Formatiert – Amazon SES verfasst und sendet eine ordnungsgemäß formatierte E-Mail-Nachricht. Sie müssen nur die „From:“- und „To:“-Adressen, einen Betreff und den Text angeben. Amazon SES übernimmt den Rest. Weitere Informationen finden Sie unter Senden einer formatierten E-Mail mit der Amazon-SES-API.
- Unformatiert – Sie verfassen und senden eine E-Mail-Nachricht manuell mit Ihren eigenen E-Mail-Headern und MIME-Typen. Wenn Sie Erfahrung mit der Formatierung Ihrer eigenen E-Mails haben, bietet Ihnen die Raw-Schnittstelle mehr Kontrolle über das Verfassen Ihrer Nachricht. Weitere Informationen finden Sie unter Senden von Roh-E-Mails mit der Amazon SES API v2.

Inhalt

- Senden einer formatierten E-Mail mit der Amazon-SES-API

- Senden von Roh-E-Mails mit der Amazon SES API v2
- Verwenden von Vorlagen zum Senden einer personalisierten E-Mail mit der Amazon-SES-API
- Senden von E-Mails über Amazon SES mithilfe eines AWS SDK
- Von Amazon SES unterstützte Inhaltskodierungen

Senden einer formatierten E-Mail mit der Amazon-SES-API

Sie können eine formatierte E-Mail senden, indem Sie das AWS-Managementkonsole oder verwenden, indem Sie die Amazon SES SES-API über eine Anwendung direkt oder indirekt über ein AWS SDK AWS Command Line Interface, das oder das AWS Tools for Windows PowerShell aufrufen.

Die Amazon-SES-API stellt die `SendEmail`-Aktion bereit, mit der Sie eine formatierte E-Mail verfassen und senden können. `SendEmail` erfordert eine Von: Adresse, An: Adresse, Nachrichtenbetreff und Nachrichtentext – Text, HTML oder beides. Weitere Informationen finden Sie unter SendEmail(API-Referenz) oder SendEmail(API v2-Referenz).

> **Note**
>
> Die E-Mail-Adresse muss eine 7-Bit-ASCII-Zeichenfolge sein. Wenn Sie E-Mails an oder von Adressen mit Unicode-Zeichen im Domänenteil der Adresse senden möchten, müssen Sie die Domäne über Punycode codieren. Weitere Informationen finden Sie unter RFC 3492.

Beispiele für die Erstellung einer formatierten Nachricht mit verschiedenen Programmiersprachen finden Sie unterCodebeispieleaus.

Tipps zur Erhöhung der E-Mail-Sendegeschwindigkeit bei mehreren `SendEmail`-Aufrufen finden Sie unter Erhöhen des Durchsatzes mit Amazon SES.

Senden von Roh-E-Mails mit der Amazon SES API v2

Sie können den Amazon SES API `SendEmail` v2-Vorgang mit dem angegebenen Inhaltstyp verwenden`raw`, um benutzerdefinierte Nachrichten im unformatierten E-Mail-Format an Ihre Empfänger zu senden.

Über E-Mail-Header-Felder

Simple Mail Transfer Protocol (SMTP) gibt an, wie E-Mail-Nachrichten gesendet werden sollen, indem der E-Mail-Umschlag und einigen seiner Parameter definiert werden. Es geht dabei aber nicht um den Inhalt der Nachricht. Stattdessen definiert das Internet-Nachrichtenformat (RFC 5322), wie die Nachricht aufgebaut werden soll.

Mit der Spezifikation für das Internet-Nachrichtenformat besteht jede E-Mail-Nachricht aus einem Header und einem Text. Der Header besteht aus Metadaten der Nachrichten und der Körper enthält die Nachricht selbst. Weitere Informationen über E-Mail-Header und -Texte finden Sie unter E-Mail-Format und Amazon SES.

Verwenden Sie die Erstellung von MIME-Nachrichten im Rohformat

Das SMTP-Protokoll war ursprünglich zum Senden von E-Mail-Nachrichten konzipiert, die nur 7-Bit-ASCII-Zeichen enthielten. Aufgrund dieser Spezifikation ist SMTP für Nicht-ASCII-Textcodierungen (z. B. Unicode), binäre Inhalte oder Anlagen unzureichend. Der Multipurpose Internet Mail Extensions-Standard (MIME) wurde entwickelt, um den Versand vieler anderer Arten von Inhalten über SMTP zu ermöglichen.

Der MIME-Standard funktioniert, indem er den Nachrichtentext in mehrere Teile unterteilt und dann angibt, wie mit den einzelnen Teilen zu verfahren ist. Beispielsweise kann ein Teil eines E-Mail-Nachrichtentext Klartext sein, während ein anderer HTML sein kann. Darüber hinaus lässt MIME zu, dass E-Mail-Nachrichten eine oder mehrere Anlagen enthalten. Die Empfänger der Nachricht können die Anlagen innerhalb ihrer E-Mail-Clients anzeigen oder die Anlagen speichern.

Der E-Mail-Header und die Inhalte werden durch eine Leerzeile getrennt. Jeder Teil der E-Mail wird durch einen Rahmen getrennt, eine Zeichenfolge, die den Anfang und das Ende jedes Teils markiert.

Die mehrteilige Nachricht im folgenden Beispiel enthält einen Text- und einen HTML-Teil sowie einen Anhang. Der Anhang sollte, wie in diesem Beispiel gezeigt, direkt unter den Anhangsüberschriften platziert werden und wird meistens in `base64` codiert.

```
From: "Sender Name" <sender@example.com>
To: recipient@example.com
Subject: Customer service contact info
Content-Type: multipart/mixed;
    boundary="a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a"

--a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
```

```
Content-Type: multipart/alternative;
    boundary="sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a"

--sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable

Please see the attached file for a list of customers to contact.

--sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
Content-Type: text/html; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable

<html>
<head></head>
<body>
<h1>Hello!</h1>
<p>Please see the attached file for a list of customers to contact.</p>
</body>
</html>

--sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a--

--a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
Content-Type: text/plain; name="customers.txt"
Content-Description: customers.txt
Content-Disposition: attachment;filename="customers.txt";
    creation-date="Sat, 05 Aug 2017 19:35:36 GMT";
Content-Transfer-Encoding: base64

SUQsRmlyc3ROYW1lLExhc3ROYW1lLENvdW50cnkKMzQ4LEpvaG4sU3RpbGVzLENhbmFkYQo5MjM4
OSxKaWUsTGl1LENoaW5hCjczNCxTaGlybGV5LFJvZHJpZ3VleixVbml0ZWQgU3RhdGVzCjI4OTMs
QW5heWEsSXllbmdhcixJbmRpYQ==

--a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a--
```

Der Inhaltstyp für die Nachricht ist `multipart/mixed`. Dieser gibt an, dass die Nachricht viele Teile hat (in diesem Beispiel einen Text und eine Anlage), und der empfangende Client muss jedes Teil getrennt handhaben.

Verschachtelt in den Körperabschnitt ist eine zweite Komponente, die den `multipart/alternative`-Inhaltstyp verwendet. Dieser Inhaltstyp gibt an, dass jedes Teil alternative Versionen desselben Inhalts enthält (in diesem Fall eine Textversion und eine HTML-Version). Wenn der E-

Mail-Client des Empfängers HTML-Inhalte anzeigen kann, dann zeigt er die HTML-Version des Textkörpers an. Wenn der E-Mail-Client des Empfängers keine HTML-Inhalte anzeigen kann, dann zeigt er die Klartextversion des Textkörpers an.

Beide Versionen der Nachricht enthalten außerdem eine Anlage (in diesem Fall eine kurze Textdatei mit einigen Kundennamen).

Wenn Sie einen MIME-Teil in einen anderen Teil verschachteln, wie in diesem Beispiel, muss das verschachtelte Teil einen `boundary`-Parameter verwenden, der sich vom `boundary`-Parameter im übergeordneten Teil unterscheidet. Diese Grenzen sollten eindeutige Zeichenfolgen sein. Zum Definieren einer Begrenzung zwischen MIME-Teilen geben Sie zwei Bindestriche (-) gefolgt von der Begrenzungszeichenfolge ein. Am Ende eines MIME-Teils platzieren Sie zwei Bindestriche am Anfang und am Ende der Begrenzungszeichenfolge.

> **Note**
>
> Eine Nachricht kann nicht mehr als 500 MIME-Teile umfassen.

MIME-Codierung

Um die Kompatibilität mit älteren Systemen zu wahren, beachtet Amazon SES die 7-Bit-ASCII-Beschränkung der SMTP-Definition in RFC 2821. Wenn Sie Inhalte senden möchten, die Nicht-ASCII-Zeichen enthalten, müssen Sie diese Zeichen in einem Format mit 7-Bit-ASCII-Zeichen formatieren.

E-Mail-Adressen

Die E-Mail-Adresse muss eine 7-Bit-ASCII-Zeichenfolge sein. Wenn Sie E-Mails an oder von Adressen mit Unicode-Zeichen im Domänenteil der Adresse senden möchten, müssen Sie die Domäne über Punycode codieren. Punycode ist weder im lokalen Teil der E-Mail-Adresse (das ist der Teil vor dem @-Zeichen) noch im "friendly from"-Namen zulässig. Wenn Sie Unicode-Zeichen im Absendernamen verwenden möchten, müssen Sie den Absendernamen mithilfe der MIME-Syntax kodieren, wie in diesem Abschnitt beschrieben. Weitere Informationen zu Punycode finden Sie unter RFC 3492.

> **Note**
>
> Diese Regel gilt nur für E-Mail-Adressen, die Sie im Umschlag der Nachricht angeben, nicht für die Nachrichten-Header. Wenn Sie den Amazon SES API `SendEmail` v2-Vorgang

verwenden, definieren die Adressen, die Sie in den `Destinations` Parametern `Source` und angeben, den Absender bzw. die Empfänger des Umschlags.

E-Mail-Header

Um eine Nachrichtenkopfzeile, oder einen Header, zu codieren, verwenden Sie MIME-codierte Wortsyntax. MIME-codierter Wortsyntax verwendet das folgende Format:

```
=?charset?encoding?encoded-text?=
```

Der Wert von *`encoding`* kann `Q` oder `B` sein. Wenn der Wert der Codierung `Q` ist, dann muss der Wert von *`encoded-text`* Q-Codierung verwenden. Wenn der Wert der Codierung `B` ist, dann muss der Wert von *`encoded-text`* base64-Codierung verwenden.

Zum Beispiel, wenn Sie die Zeichenfolge „Як ти поживаєш?“ verwenden möchten In der Betreffzeile einer E-Mail können Sie eine der folgenden Codierungen verwenden:

- Q-Codierung

```
=?utf-8?Q?
=D0=AF=D0=BA_=D1=82=D0=B8_=D0=BF=D0=BE=D0=B6=D0=B8=D0=B2=D0=B0=D1=94=D1=88=3F?=
```

- Base64-Codierung

```
=?utf-8?B?0K/QuiDRgtC4INC/0L7QttC40LLQsNGU0Yg/?=
```

Weitere Informationen zur Q_Codierung finden Sie unter RFC 2047. Weitere Informationen zur base64-Codierung finden Sie unter RFC 2045.

Nachrichtentext

Um den Nachrichtentext zu codieren, können Sie Quoted-Printable-Codierung oder base64-Codierung verwenden. Verwenden Sie danach den `Content-Transfer-Encoding`-Header, um anzugeben, welche Codierungsschema Sie verwendet haben.

Angenommen, der Text Ihrer Nachricht enthält den folgenden Text:

१९७२ मे रे टॉमलंसिन ने पहला ई-मेल सेंदश भेजा | रे टॉमलंसिन ने ही स्रव्परथम @ चन्हि का चयन कयिा और इनही को ईमल का आवष्किारक माना जाता है

Wenn Sie diesen Text mit base64-Codierung codieren, geben Sie zuerst den folgenden Header ein:

```
Content-Transfer-Encoding: base64
```

Schließen Sie dann im Körperabschnitt der E-Mail den base64-codierten Text ein:

```
4KWn4KWv4KWt4KWoIOCkruClhyDgpLDgpYcg4KSf4KWJ4KSu4KSy4KS/4KSC4KS44KSoIOCkqOCl
hyDgpKrgpLngpLLgpL4g4KSILeCkruClh+CksiDgpLjgpILgpKbgpYfgpLYg4KSt4KWH4KSc4KS+
IHwg4KSw4KWHIOCkn+ClieCkruCksuCkv+CkguCkuOCkqCDgpKjgpYcg4KS54KWAIOCkuOCksOCl
jeCkteCkquCljeCksOCkpeCkriBAIOCkmuCkv+CkqOCljeCkuSDgpJXgpL4g4KSa4KSv4KSoIOCk
leCkv+Ckr+CkviDgpJTgpLAg4KSH4KSo4KWN4KS54KWAIOCkleCliyDgpIjgpK7gpYfgpLIg4KSV
4KS+IOCkhuCkteCkv+Ckt+CljeCkleCkvuCksOCklSDgpK7gpL7gpKjgpL4g4KSc4KS+4KSk4KS+
IOCkueCliAo=
```

> **Note**
>
> In einigen Fällen können Sie in mit Amazon SES gesendeten Nachrichten das 8-Bit `Content-Transfer-Encoding` verwenden. Wenn Amazon SES jedoch Änderungen an Ihren Nachrichten vornehmen muss (wenn Sie z. B. Öffnungs- und Klicknachverfolgung verwenden), wird der 8-Bit-codierte Inhalt möglicherweise nicht richtig angezeigt, wenn er im Postfach der Empfänger eingeht. Aus diesem Grund sollten Sie Inhalte, die sich nicht im 7-Bit-ASCII-Format befinden, immer codieren.

Dateianhänge

Um eine Datei an eine E-Mail anfügen zu können, müssen Sie die Anlage mit base64-Codierung codieren. Anlagen werden in der Regel in dedizierten MIME-Nachrichtenteilen platziert. Dazu gehören die folgenden Header:

- Inhaltstyp – der Dateityp der Anlage. Hier sind einige Beispiele für häufige MIME-Inhaltstyp-Deklarationen:
  - Reine Textdatei – `Content-Type: text/plain; name="sample.txt"`
  - Microsoft Word-Dokument – `Content-Type: application/msword; name="document.docx"`
  - JPG-Bild – `Content-Type: image/jpeg; name="photo.jpeg"`
- Inhaltsanordnung – gibt an, wie der E-Mail-Client des Empfängers die Inhalte anordnen soll. Für Anlagen ist dieser Wert `Content-Disposition: attachment`.

- Inhaltsübertragungscodierung – das Schema, das zum Codieren der Anlage verwendet wurde. Für Dateianlagen ist dieser Wert fast immer `base64`.
- Der codierte Anhang – Sie müssen den eigentlichen Anhang, wie im Beispiel gezeigt, codieren und ihn in den Text unter den Anhangsüberschriften einfügen.

Amazon SES akzeptiert die gängigsten Dateitypen. Eine Liste der Dateitypen, die Amazon SES nicht akzeptiert, finden Sie unter SES unterstützt nicht die Typen von Anhängen.

Senden von Roh-E-Mails mit der Amazon SES API v2

Die Amazon SES API v2 bietet die `SendEmail` Aktion, mit der Sie eine E-Mail-Nachricht in dem Format verfassen und senden können, das Sie angeben, wenn Sie den Inhaltstyp auf Einfach, Rohformat oder Vorlage festlegen. Eine vollständige Beschreibung finden Sie unter `SendEmail`. Im folgenden Beispiel wird der Inhaltstyp für `raw` das Senden von Nachrichten im unformatierten E-Mail-Format angegeben.

> **Note**
>
> Tipps zur Erhöhung der E-Mail-Sendegeschwindigkeit bei mehreren `SendEmail`-Aufrufen finden Sie unter Erhöhen des Durchsatzes mit Amazon SES.

Der Nachrichtentext muss eine ordnungsgemäß formatierte Raw-E-Mail-Nachricht mit entsprechenden Header-Feldern und Nachrichtentext-Codierung enthalten. Obwohl es möglich ist, die unformatierte Nachricht manuell in einer Anwendung zu verfassen, ist es wesentlich einfacher, dies mithilfe von vorhandenen E-Mail-Bibliotheken zu tun.

Java

Das folgende Codebeispiel zeigt, wie Sie die JavaMailBibliothek verwenden und eine Roh-E-Mail verfassen und versenden. AWS SDK für Java

```
package com.amazonaws.samples;

import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.io.PrintStream;
import java.nio.ByteBuffer;
import java.util.Properties;
```

```
// JavaMail libraries. Download the JavaMail API
// from https://javaee.github.io/javamail/
import javax.activation.DataHandler;
import javax.activation.DataSource;
import javax.activation.FileDataSource;
import javax.mail.Message;
import javax.mail.MessagingException;
import javax.mail.Session;
import javax.mail.internet.AddressException;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeBodyPart;
import javax.mail.internet.MimeMessage;
import javax.mail.internet.MimeMultipart;

// AWS SDK libraries. Download the AWS SDK für Java // from https://aws.amazon.com/
sdk-for-java
import com.amazonaws.regions.Regions;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailService;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailServiceClientBuilder;
import com.amazonaws.services.simpleemail.model.RawMessage;
import com.amazonaws.services.simpleemail.model.SendRawEmailRequest;

public class AmazonSESSample {

 // Replace sender@example.com with your "From" address.
 // This address must be verified with Amazon SES.
 private static String SENDER = "Sender Name <sender@example.com>";

 // Replace recipient@example.com with a "To" address. If your account
 // is still in the sandbox, this address must be verified.
 private static String RECIPIENT = "recipient@example.com";

 // Specify a configuration set. If you do not want to use a configuration
 // set, comment the following variable, and the
 // ConfigurationSetName=CONFIGURATION_SET argument below.
 private static String CONFIGURATION_SET = "ConfigSet";

 // The subject line for the email.
 private static String SUBJECT = "Customer service contact info";

 // The full path to the file that will be attached to the email.
 // If you're using Windows, escape backslashes as shown in this variable.
 private static String ATTACHMENT = "C:\\Users\\sender\\customers-to-contact.xlsx";
```

```
// The email body for recipients with non-HTML email clients.
private static String BODY_TEXT = "Hello,\r\n"
                                        + "Please see the attached file for a list "
                                        + "of customers to contact.";

// The HTML body of the email.
private static String BODY_HTML = "<html>"
                                        + "<head></head>"
                                        + "<body>"
                                        + "<h1>Hello!</h1>"
                                        + "<p>Please see the attached file for a "
                                        + "list of customers to contact.</p>"
                                        + "</body>"
                                        + "</html>";

   public static void main(String[] args) throws AddressException,
MessagingException, IOException {

    Session session = Session.getDefaultInstance(new Properties());

       // Create a new MimeMessage object.
       MimeMessage message = new MimeMessage(session);

       // Add subject, from and to lines.
       message.setSubject(SUBJECT, "UTF-8");
       message.setFrom(new InternetAddress(SENDER));
       message.setRecipients(Message.RecipientType.TO,
InternetAddress.parse(RECIPIENT));

       // Create a multipart/alternative child container.
       MimeMultipart msg_body = new MimeMultipart("alternative");

       // Create a wrapper for the HTML and text parts.
       MimeBodyPart wrap = new MimeBodyPart();

       // Define the text part.
       MimeBodyPart textPart = new MimeBodyPart();
       textPart.setContent(BODY_TEXT, "text/plain; charset=UTF-8");

       // Define the HTML part.
       MimeBodyPart htmlPart = new MimeBodyPart();
       htmlPart.setContent(BODY_HTML,"text/html; charset=UTF-8");
```

```
        // Add the text and HTML parts to the child container.
        msg_body.addBodyPart(textPart);
        msg_body.addBodyPart(htmlPart);

        // Add the child container to the wrapper object.
        wrap.setContent(msg_body);

        // Create a multipart/mixed parent container.
        MimeMultipart msg = new MimeMultipart("mixed");

        // Add the parent container to the message.
        message.setContent(msg);

        // Add the multipart/alternative part to the message.
        msg.addBodyPart(wrap);

        // Define the attachment
        MimeBodyPart att = new MimeBodyPart();
        DataSource fds = new FileDataSource(ATTACHMENT);
        att.setDataHandler(new DataHandler(fds));
        att.setFileName(fds.getName());

        // Add the attachment to the message.
        msg.addBodyPart(att);

        // Try to send the email.
        try {
            System.out.println("Attempting to send an email through Amazon SES "
                               +"using the AWS SDK for Java...");

            // Instantiate an Amazon SES client, which will make the service
            // call with the supplied AWS credentials.
            AmazonSimpleEmailService client =
                    AmazonSimpleEmailServiceClientBuilder.standard()
                    // Replace US_WEST_2 with the AWS Region you're using for
                    // Amazon SES.
                    .withRegion(Regions.US_WEST_2).build();

            // Print the raw email content on the console
            PrintStream out = System.out;
            message.writeTo(out);

            // Send the email.
            ByteArrayOutputStream outputStream = new ByteArrayOutputStream();
```

```
            message.writeTo(outputStream);
            RawMessage rawMessage =
              new RawMessage(ByteBuffer.wrap(outputStream.toByteArray()));

            SendRawEmailRequest rawEmailRequest =
              new SendRawEmailRequest(rawMessage)
                  .withConfigurationSetName(CONFIGURATION_SET);

            client.sendRawEmail(rawEmailRequest);
            System.out.println("Email sent!");
        // Display an error if something goes wrong.
        } catch (Exception ex) {
          System.out.println("Email Failed");
            System.err.println("Error message: " + ex.getMessage());
            ex.printStackTrace();
        }
    }
}
```

Python

Das folgende Codebeispiel veranschaulicht, wie Sie mit Python email.mime-Paketen und dem AWS SDK für Python (Boto) eine Raw-E-Mail erstellen und senden können.

```
import json
import boto3
from botocore.exceptions import ClientError
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
from email.mime.application import MIMEApplication
import os

def boto3_rawemailv2():
    SENDER = "Sender <sender@example.com>"
    RECIPIENT = "recipient@example.com"
    CONFIGURATION_SET = "ConfigSet"
    AWS_REGION = "us-east-1"
    SUBJECT = "Customer service contact info"
    ATTACHMENT = "path/to/customers-to-contact.xlsx"
    BODY_TEXT = "Hello,\r\nPlease see the attached file for a list of customers to
 contact."

    # The HTML body of the email.
```

```
    BODY_HTML = """\
    <html>
    <head/>
    <body>
    <h1>Hello!</h1>
    <p>Please see the attached file for a list of customers to contact.</p>
    </body>
    </html>
    """

    # The character encoding for the email.
    CHARSET = "utf-8"
    msg = MIMEMultipart('mixed')
    # Add subject, from and to lines.
    msg['Subject'] = SUBJECT
    msg['From'] = SENDER
    msg['To'] = RECIPIENT

    # Create a multipart/alternative child container.
    msg_body = MIMEMultipart('alternative')

    # Encode the text and HTML content and set the character encoding. This step is
    # necessary if you're sending a message with characters outside the ASCII range.
    textpart = MIMEText(BODY_TEXT.encode(CHARSET), 'plain', CHARSET)
    htmlpart = MIMEText(BODY_HTML.encode(CHARSET), 'html', CHARSET)

    # Add the text and HTML parts to the child container.
    msg_body.attach(textpart)
    msg_body.attach(htmlpart)

    # Define the attachment part and encode it using MIMEApplication.
    att = MIMEApplication(open(ATTACHMENT, 'rb').read())

    # Add a header to tell the email client to treat this part as an attachment,
    # and to give the attachment a name.
    att.add_header('Content-
Disposition','attachment',filename=os.path.basename(ATTACHMENT))

    # Attach the multipart/alternative child container to the multipart/mixed
    # parent container.
    msg.attach(msg_body)
    msg.attach(att)

    #changes start from here
```

```
    strmsg = str(msg)
    body = bytes (strmsg, 'utf-8')




    client = boto3.client('sesv2')
    response = client.send_email(
    FromEmailAddress=SENDER,
    Destination={
        'ToAddresses': [RECIPIENT]
    },
    Content={
        'Raw': {
            'Data': body
        }
    }
    )
    print(response)
boto3_rawemailv2 ()
```

Verwenden von Vorlagen zum Senden einer personalisierten E-Mail mit der Amazon-SES-API

In Amazon SES können Sie E-Mails mit Vorlagen entweder mithilfe einer gespeicherten Vorlage oder mithilfe einer Inline-Vorlage versenden.

- Gespeicherte Vorlage — Bezieht sich auf die `Template`Ressource, die mithilfe des `CreateEmailTemplate` Vorgangs in der Amazon SES v2-API in SES erstellt und gespeichert wird. Die Vorlage enthält den Betreff und den Text der E-Mail mit Variablen (Platzhaltern), die dem geschriebenen Inhalt entsprechen. Der Name der gespeicherten Vorlage und die dynamischen Daten für die Platzhaltervariablen in der Vorlage werden beim Aufrufen der API-Operationen `SendEmail` oder der `SendBulkEmail` v2-API-Operation bereitgestellt.

  Gespeicherte Vorlagen können einfach wiederverwendet werden und können Ihnen Zeit und Mühe beim Senden ähnlicher Arten von E-Mails sparen. Anstatt jede E-Mail von Grund auf neu zu erstellen, müssen Sie die Basisstruktur und das Design nur einmal erstellen und dann einfach den dynamischen Inhalt innerhalb der Vorlage aktualisieren.

- Inline-Vorlage — Die `Template` Ressource wird nicht verwendet, sondern der Betreff und der Text der E-Mail, die Variablen (Platzhalter) enthält, werden zusammen mit den Werten für diese Platzhaltervariablen bereitgestellt, wenn entweder die API-Operationen `SendEmail` oder die `SendBulkEmail` v2-API-Operationen aufgerufen werden.

  Inline-Vorlagen optimieren den Prozess für den Versand von Massen-E-Mails, indem sie die Verwaltung von Vorlagenressourcen in Ihrem SES-Konto überflüssig machen und den Integrationsprozess vereinfachen, indem Sie Vorlageninhalte direkt in Ihre Anwendungslogik aufnehmen können. Sie werden nicht auf das Limit von 20.000 Vorlagen pro Vorlage angerechnet. AWS-Region

Bei der Verwendung von gespeicherten Vorlagen gelten die folgenden Grenzwerte:

- Sie können jeweils bis zu 20.000 E-Mail-Vorlagen erstellen AWS-Region.
- Jede Vorlage kann bis zu 500 KB groß sein, einschließlich Text- und HTML-Teile.

Bei der Verwendung von Inline-Vorlagen gilt das folgende Limit:

- Jede JSON-Eingabedatei kann bis zu 1 MB groß sein, einschließlich der Text- und HTML-Teile.

Folgendes gilt sowohl für gespeicherte als auch für Inline-Vorlagen:

- Die Anzahl der Ersatzvariablen, die verwendet werden können, ist unbegrenzt.
- Sie können bei jedem Aufruf des `SendBulkEmail` Vorgangs E-Mails an bis zu 50 Zielobjekte senden. Das `Destination`Objekt kann mehrere Empfänger enthalten, die in ToAddressesCcAddresses, und definiert sind BccAddresses. Die Anzahl der Ziele, die Sie mit einem einzigen Aufruf der v2-API kontaktieren können, ist möglicherweise durch die maximale Senderate Ihres Kontos begrenzt. Weitere Informationen finden Sie unter Verwalten Ihrer Amazon SES Versandkontingente.

Dieses Kapitel enthält Verfahren mit Beispielen für die Verwendung sowohl gespeicherter Vorlagen als auch Inline-Vorlagen.

> **Note**
>
> Bei diesen Verfahren wird vorausgesetzt, dass Sie die AWS CLI bereits installiert und konfiguriert haben. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

(Optional) Teil 1: Richten Sie Benachrichtigungen über Ereignisse bei Rendering-Fehlern ein

Wenn Sie eine E-Mail versenden, die ungültige Personalisierungsinhalte enthält, akzeptiert Amazon SES die Nachricht möglicherweise, kann sie jedoch nicht zustellen. Wenn Sie personalisierte E-Mails versenden möchten, sollten Sie SES daher so konfigurieren, dass Rendering-Fehler-Ereignisbenachrichtigungen über Amazon SNS gesendet werden. Wenn Sie eine Benachrichtigung über ein Rendering-Fehlerereignis erhalten, können Sie feststellen, welche Nachricht den ungültigen Inhalt enthalten hat, die Probleme beheben und die Nachricht erneut senden.

Das Verfahren in diesem Abschnitt ist optional, wird aber dringend empfohlen.

So konfigurieren Sie Benachrichtigungen über Rendering-Fehlerereignisse

1. Erstellen Sie ein Amazon-SNS-Thema. Anweisungen finden Sie unter Erstellen eines Themas im Amazon-Simple-Notification-Service-Entwicklerhandbuch.
2. Abonnieren Sie das Amazon-SNS-Thema. Beispiel: Wenn Sie Rendering-Fehlerbenachrichtigungen per E-Mail empfangen möchten, abonnieren Sie einen E-Mail-Endpunkt für das Thema.

   Anweisungen finden Sie unter Abonnieren eines Themas im Amazon Simple-Notification-Service-Entwicklerhandbuch.
3. Führen Sie das Verfahren unter the section called “Einrichten eines Amazon SNS-Ereignisziels ” durch, um Ihre Konfigurationssätze zum Veröffentlichen von Rendering-Fehlerereignissen in Ihrem Amazon-SNS-Thema zu erstellen.

(Optional) Teil 2: Erstellen Sie eine E-Mail-Vorlage

Wenn Sie beabsichtigen, eine gespeicherte Vorlage zu verwenden, erfahren Sie in diesem Abschnitt, wie Sie die Vorlage mithilfe des `CreateEmailTemplate`SES v2-API-Vorgangs erstellen. Sie können diesen Schritt überspringen, wenn Sie eine Inline-Vorlage verwenden möchten.

Bei diesem Verfahren wird vorausgesetzt, dass Sie die AWS CLI bereits installiert und konfiguriert haben. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

So erstellen Sie die Vorlage

1. Erstellen Sie in einem Texteditor eine neue Datei und fügen Sie den folgenden Code ein, um sie nach Bedarf anzupassen.

```
{
    "TemplateName": "MyTemplate",
    "TemplateContent": {
        "Subject": "Greetings, {{name}}!",
        "Text": "Dear {{name}},\r\nYour favorite animal is {{favoriteanimal}}.",
        "Html": "<h1>Hello {{name}},</h1><p>Your favorite animal is
 {{favoriteanimal}}.</p>"
    }
}
```

   Dieser Code enthält die folgenden Eigenschaften:

   - TemplateName— Der Name der `Template` Ressource. Beim Senden der E-Mail-Adresse beziehen Sie sich auf diesen Namen.
   - TemplateContent— Ein Container für die folgenden Attribute:
     - Betreff – Die Betreffzeile der E-Mail. Diese Eigenschaft kann Ersatz-Tags enthalten. Diese Tags verwenden das folgende Format: `{{tagname}}`. Wenn Sie die E-Mail senden, können Sie einen Wert für `tagname` für jede Zieladresse angeben.
     - Html — Der HTML-Text der E-Mail. Diese Eigenschaft kann Ersatz-Tags enthalten. Das vorherige Beispiel umfasst zwei Tags: `{{name}}` und `{{favoriteanimal}}`.
     - Text — Der Textkörper der E-Mail. Empfänger, deren E-Mail-Clients keine HTML-Inhalte anzeigen, sehen diese Version der E-Mail. Diese Eigenschaft kann auch Ersatz-Tags enthalten.
2. Passen Sie das vorherige Beispiel an Ihre Bedürfnisse an und speichern Sie dann die Datei als *`mytemplate.json`*.
3. Geben Sie in der Befehlszeile den folgenden Befehl ein, um mithilfe der `CreateEmailTemplate`v2-API-Operation eine neue Vorlage zu erstellen:

```
aws sesv2 create-email-template --cli-input-json file://mytemplate.json
```

Teil 3: Senden der personalisierten E-Mail

Sie können die folgenden beiden SES v2-API-Operationen verwenden, um E-Mails entweder mithilfe von gespeicherten Vorlagen oder Inline-Vorlagen zu versenden:

- Der `SendEmail`Vorgang ist nützlich, um eine benutzerdefinierte E-Mail an ein einzelnes Zielobjekt zu senden. Das `Destination`v2-API-Objekt kann die BccAddressesEigenschaften ToAddressesCcAddresses, und enthalten. Diese können in beliebiger Kombination verwendet werden und können eine oder mehrere E-Mail-Adressen enthalten, an die dieselbe E-Mail gesendet wird.
- Der `SendBulkEmail`Vorgang ist nützlich, um in einem einzigen Aufruf der v2-API eindeutige E-Mails an mehrere Zielobjekte zu senden.

Dieser Abschnitt enthält Beispiele für die Verwendung von AWS CLI zum Senden von E-Mails mit Vorlagen mithilfe dieser beiden Sendevorgänge.

Senden von E-Mail-Vorlagen an ein einzelnes Zielobjekt

Sie können den `SendEmail`Vorgang verwenden, um eine E-Mail an einen oder mehrere Empfänger zu senden, die in einem einzigen Zielobjekt definiert sind. Alle Empfänger im `Destination`-Objekt erhalten dieselbe E-Mail.

Um eine E-Mail mit einer Vorlage an ein einzelnes Zielobjekt zu senden

1. Je nachdem, ob Sie eine gespeicherte Vorlage oder eine Inline-Vorlage verwenden möchten, wählen Sie das entsprechende Codebeispiel aus, um es in einen Texteditor einzufügen, und passen Sie es nach Bedarf an.

   Stored template code example

   Beachten Sie, dass die Vorlage, die Sie im vorherigen Schritt erstellt haben MyTemplate, als Wert für den `TemplateName` Parameter referenziert wird.

   ```
   {
       "FromEmailAddress": "Mary Major <mary.major@example.com>",
       "Destination": {
   ```

```
        "ToAddresses": [
            "alejandro.rosalez@example.com", "jimmy.jet@example.com"
        ]
    },
    "Content": {
        "Template": {
            "TemplateName": "MyTemplate",
            "TemplateData": "{ \"name\":\"Alejandro\", \"favoriteanimal\":
 \"alligator\" }"
        }
    },
    "ConfigurationSetName": "ConfigSet"
}
```

Dieser Code enthält die folgenden Eigenschaften:

- FromEmailAddress— Die E-Mail-Adresse des Absenders.
- Ziel — Ein Objekt, das die in den BccAddressesEigenschaften ToAddressesCcAddresses, und definierten E-Mail-Empfänger enthält. Diese können in beliebiger Kombination verwendet werden und können eine oder mehrere E-Mail-Adressen enthalten, an die dieselbe E-Mail gesendet wird.
- TemplateName— Der Name der `Template` Ressource, die auf die E-Mail angewendet werden soll.
- TemplateData— Eine maskierte JSON-Zeichenfolge, die Schlüssel-Wert-Paare enthält. Die Schlüssel entsprechen den Variablen, die in den `TemplateContent` Eigenschaften der gespeicherten Vorlage definiert sind, zum Beispiel. `{{name}}` Die Werte stellen den Inhalt dar, der die Variablen ersetzt.
- ConfigurationSetName— Der Name des Konfigurationssatzes, der beim Senden der E-Mail verwendet werden soll.

> **Note**
>
> Wir empfehlen, einen Konfigurationssatz zu verwenden, der zum Veröffentlichen von Rendering-Fehlerereignissen in Amazon SNS konfiguriert ist. Weitere Informationen finden Sie unter the section called “(Optional) Teil 1: Benachrichtigungen einrichten”.

Inline template code example

Beachten Sie, dass die `TemplateContent` Eigenschaften (die normalerweise in einer gespeicherten Vorlage definiert würden) zusammen mit der `TemplateData` Eigenschaft inline definiert werden, wodurch diese Vorlage zu einer Inline-Vorlage wird.

```
{
    "FromEmailAddress": "Mary Major <mary.major@example.com>",
    "Destination": {
        "ToAddresses": [
            "alejandro.rosalez@example.com", "jimmy.jet@example.com"
        ]
    },
    "Content": {
        "Template": {
            "TemplateContent": {
                "Subject": "Greetings, {{name}}!",
                "Text": "Dear {{name}},\r\nYour favorite animal is
 {{favoriteanimal}}.",
                "Html": "<h1>Hello {{name}},</h1><p>Your favorite animal is
 {{favoriteanimal}}.</p>"
            },
            "TemplateData": "{ \"name\":\"Alejandro\", \"favoriteanimal\":
 \"alligator\" }"
        }
    },
    "ConfigurationSetName": "ConfigSet"
}
```

Dieser Code enthält die folgenden Eigenschaften:

- FromEmailAddress— Die E-Mail-Adresse des Absenders.
- Ziel — Ein Objekt, das die in den BccAddressesEigenschaften ToAddressesCcAddresses, und definierten E-Mail-Empfänger enthält. Diese können in beliebiger Kombination verwendet werden und können eine oder mehrere E-Mail-Adressen enthalten, an die dieselbe E-Mail gesendet wird.
- TemplateContent— Ein Container für die folgenden Attribute:

    - Betreff – Die Betreffzeile der E-Mail. Diese Eigenschaft kann Ersatz-Tags enthalten. Diese Tags verwenden das folgende Format: `{{tagname}}`. Wenn Sie die E-Mail senden, können Sie einen Wert für `tagname` für jede Zieladresse angeben.
    - Html — Der HTML-Text der E-Mail. Diese Eigenschaft kann Ersatz-Tags enthalten. Das vorherige Beispiel umfasst zwei Tags: `{{name}}` und `{{favoriteanimal}}`.
    - Text — Der Textkörper der E-Mail. Empfänger, deren E-Mail-Clients keine HTML-Inhalte anzeigen, sehen diese Version der E-Mail. Diese Eigenschaft kann auch Ersatz-Tags enthalten.
- TemplateData— Eine maskierte JSON-Zeichenfolge, die Schlüssel-Wert-Paare enthält. Die Schlüssel entsprechen den Variablen, die in den `TemplateContent` Eigenschaften in dieser Datei definiert sind, zum Beispiel. `{{name}}` Die Werte stellen den Inhalt dar, der die Variablen ersetzt.
- ConfigurationSetName— Der Name des Konfigurationssatzes, der beim Senden der E-Mail verwendet werden soll.

> **Note**
>
> Wir empfehlen, einen Konfigurationssatz zu verwenden, der zum Veröffentlichen von Rendering-Fehlerereignissen in Amazon SNS konfiguriert ist. Weitere Informationen finden Sie unter the section called “(Optional) Teil 1: Benachrichtigungen einrichten”.

2. Passen Sie das vorherige Beispiel an Ihre Bedürfnisse an und speichern Sie dann die Datei als *myemail.json*.
3. Geben Sie in der Befehlszeile den folgenden v2-API-Befehl ein, um die E-Mail zu senden:

```
aws sesv2 send-email --cli-input-json file://myemail.json
```

Senden von E-Mails mit Vorlagen an mehrere Zielobjekte

Sie können den `SendBulkEmail`Vorgang verwenden, um in einem einzigen Aufruf der SES v2-API eine E-Mail an mehrere Zielobjekte zu senden. SES sendet eine eindeutige E-Mail an den oder die Empfänger in jedem `Destination`Objekt.

Um eine E-Mail mit einer Vorlage an mehrere Zielobjekte zu senden

1. Je nachdem, ob Sie eine gespeicherte Vorlage oder eine Inline-Vorlage verwenden möchten, wählen Sie das entsprechende Codebeispiel aus, um es in einen Texteditor einzufügen, und passen Sie es nach Bedarf an.

   Stored template code example

   Beachten Sie, dass die Vorlage, die Sie im vorherigen Schritt erstellt haben MyTemplate, als Wert für den `TemplateName` Parameter referenziert wird.

```
{
    "FromEmailAddress": "Mary Major <mary.major@example.com>",
    "DefaultContent": {
        "Template": {
            "TemplateName": "MyTemplate",
            "TemplateData": "{ \"name\":\"friend\", \"favoriteanimal\":\"unknown
\" }"
        }
    },
    "BulkEmailEntries": [
        {
            "Destination": {
                "ToAddresses": [
                    "anaya.iyengar@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{ \"name\":\"Anaya\",
 \"favoriteanimal\":\"angelfish\" }"
                }
            }
        },
        {
            "Destination": {
                "ToAddresses": [
                    "liu.jie@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
```

```
                    "ReplacementTemplateData": "{ \"name\":\"Liu\",
 \"favoriteanimal\":\"lion\" }"
                }
            }
        },
        {
            "Destination": {
                "ToAddresses": [
                    "shirley.rodriguez@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{ \"name\":\"Shirley\",
 \"favoriteanimal\":\"shark\" }"
                }
            }
        },
        {
            "Destination": {
                "ToAddresses": [
                    "richard.roe@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{}"
                }
            }
        }
    ],
    "ConfigurationSetName": "ConfigSet"
}
```

Dieser Code enthält die folgenden Eigenschaften:

- FromEmailAddress— Die E-Mail-Adresse des Absenders.
- DefaultContent— Ein JSON-Objekt, das die `TemplateData` Objekte `TemplateName` und enthält.
- TemplateName— Der Name der `Template` Ressource, die auf die E-Mail angewendet werden soll.

- TemplateData— Enthält Schlüssel-Wert-Paare, die verwendet werden, wenn das `ReplacementEmailContent` Objekt ein leeres JSON-Objekt,`{}`, in der `ReplacementTemplateData` Eigenschaft enthält.
- BulkEmailEntries— Ein Array, das ein oder mehrere `Destination` Objekte enthält.
- Ziel — Ein Objekt, das die in den BccAddressesEigenschaften ToAddressesCcAddresses, und definierten E-Mail-Empfänger enthält. Diese können in beliebiger Kombination verwendet werden und können eine oder mehrere E-Mail-Adressen enthalten, an die dieselbe E-Mail gesendet wird.
- ReplacementTemplateData— Eine maskierte JSON-Zeichenfolge, die Schlüssel-Wert-Paare enthält. Die Schlüssel entsprechen den Variablen in der Vorlage, zum Beispiel. `{{name}}` Die Werte stellen den Inhalt dar, der die Variablen in der E-Mail ersetzt. (Wenn die JSON-Zeichenfolge hier leer ist, was durch angezeigt wird`{}`, werden die Schlüssel-Wert-Paare verwendet, die in der `TemplateData` Eigenschaft innerhalb des `DefaultContent` Objekts definiert sind.)
- ConfigurationSetName— Der Name des Konfigurationssatzes, der beim Senden der E-Mail verwendet werden soll.

> **Note**
>
> Wir empfehlen, einen Konfigurationssatz zu verwenden, der zum Veröffentlichen von Rendering-Fehlerereignissen in Amazon SNS konfiguriert ist. Weitere Informationen finden Sie unter the section called “(Optional) Teil 1: Benachrichtigungen einrichten”.

Inline template code example

Beachten Sie, dass die `TemplateContent` Eigenschaften (die normalerweise in einer gespeicherten Vorlage definiert würden) zusammen mit der `TemplateData` Eigenschaft inline definiert werden, wodurch diese Vorlage zu einer Inline-Vorlage wird.

```
{
    "FromEmailAddress": "Mary Major <mary.major@example.com>",
    "DefaultContent": {
        "Template": {
            "TemplateContent": {
                "Subject": "Greetings, {{name}}!",
```

```
                "Text": "Dear {{name}},\r\nYour favorite animal is
 {{favoriteanimal}}.",
                "Html": "<h1>Hello {{name}},</h1><p>Your favorite animal is
 {{favoriteanimal}}.</p>"
            },
            "TemplateData": "{ \"name\":\"friend\", \"favoriteanimal\":\"unknown
\" }"
        }
    },
    "BulkEmailEntries": [
        {
            "Destination": {
                "ToAddresses": [
                    "anaya.iyengar@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{ \"name\":\"Anaya\",
 \"favoriteanimal\":\"angelfish\" }"
                }
            }
        },
        {
            "Destination": {
                "ToAddresses": [
                    "liu.jie@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{ \"name\":\"Liu\",
 \"favoriteanimal\":\"lion\" }"
                }
            }
        },
        {
            "Destination": {
                "ToAddresses": [
                    "shirley.rodriguez@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
```

```
                    "ReplacementTemplateData": "{ \"name\":\"Shirley\",
\"favoriteanimal\":\"shark\" }"
                }
            }
        },
        {
            "Destination": {
                "ToAddresses": [
                    "richard.roe@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{}"
                }
            }
        }
    ],
    "ConfigurationSetName": "ConfigSet"
}
```

Dieser Code enthält die folgenden Eigenschaften:

- FromEmailAddress— Die E-Mail-Adresse des Absenders.
- DefaultContent— Ein JSON-Objekt, das die `TemplateData` Objekte `TemplateContent` und enthält.
- TemplateContent— Ein Container für die folgenden Attribute:
  - Betreff – Die Betreffzeile der E-Mail. Diese Eigenschaft kann Ersatz-Tags enthalten. Diese Tags verwenden das folgende Format: `{{tagname}}`. Wenn Sie die E-Mail senden, können Sie einen Wert für `tagname` für jede Zieladresse angeben.
  - Html — Der HTML-Text der E-Mail. Diese Eigenschaft kann Ersatz-Tags enthalten. Das vorherige Beispiel umfasst zwei Tags: `{{name}}` und `{{favoriteanimal}}`.
  - Text — Der Textkörper der E-Mail. Empfänger, deren E-Mail-Clients keine HTML-Inhalte anzeigen, sehen diese Version der E-Mail. Diese Eigenschaft kann auch Ersatz-Tags enthalten.
- TemplateData— Enthält Schlüssel-Wert-Paare, die verwendet werden, wenn das `ReplacementEmailContent` Objekt ein leeres JSON-Objekt,`{}`, in der `ReplacementTemplateData` Eigenschaft enthält.
- BulkEmailEntries— Ein Array, das ein oder mehrere `Destination` Objekte enthält.

- Ziel — Ein Objekt, das die in den BccAddressesEigenschaften ToAddressesCcAddresses, und definierten E-Mail-Empfänger enthält. Diese können in beliebiger Kombination verwendet werden und können eine oder mehrere E-Mail-Adressen enthalten, an die dieselbe E-Mail gesendet wird.
- ReplacementTemplateData— Eine maskierte JSON-Zeichenfolge, die Schlüssel-Wert-Paare enthält. Die Schlüssel entsprechen den Variablen, die in den `TemplateContent` Eigenschaften in dieser Datei definiert sind, zum Beispiel. `{{name}}` Die Werte stellen den Inhalt dar, der die Variablen in der E-Mail ersetzt. (Wenn die JSON-Zeichenfolge hier leer ist, was durch angezeigt wird`{}`, werden die in der `TemplateData` Eigenschaft innerhalb des `DefaultContent` Objekts definierten Schlüssel-Wert-Paare verwendet.)
- ConfigurationSetName— Der Name des Konfigurationssatzes, der beim Senden der E-Mail verwendet werden soll.

> **Note**
>
> Wir empfehlen, einen Konfigurationssatz zu verwenden, der zum Veröffentlichen von Rendering-Fehlerereignissen in Amazon SNS konfiguriert ist. Weitere Informationen finden Sie unter the section called “(Optional) Teil 1: Benachrichtigungen einrichten”.

2. Ändern Sie die Werte im obigen Code Ihren Bedürfnissen entsprechend ab, und speichern Sie die Datei anschließend unter *`mybulkemail.json`*.
3. Geben Sie in der Befehlszeile den folgenden v2-API-Befehl ein, um die Massen-E-Mail zu senden:

```
aws sesv2 send-bulk-email --cli-input-json file://mybulkemail.json
```

Erweiterte E-Mail-Personalisierung

Wenn Sie eine gespeicherte Vorlage verwenden, d. h. eine `Template`Ressource in Amazon SES mithilfe des `CreateEmailTemplate` Vorgangs mit der SES v2-API erstellt haben, können Sie das Handlebars-System nutzen, um Vorlagen zu erstellen, die erweiterte Funktionen wie verschachtelte Attribute, Array-Iteration, grundlegende bedingte Anweisungen und die Erstellung von Inline-Partials enthalten. Dieser Abschnitt enthält Beispiele für diese Funktionen.

Handlebars umfasst neben den in diesem Abschnitt vorgestellten Funktionen noch weitere Funktionen. Weitere Informationen finden Sie unter Built-in Helpers auf handlebarsjs.com.

> **Note**
>
> SES entgeht dem HTML-Inhalt beim Rendern der HTML-Vorlage für eine Nachricht nicht. Dies bedeutet, dass Sie, wenn Sie vom Benutzer eingegebene Daten, z. B. aus einem Kontaktformular, einbeziehen, diese auf der Client-Seite entfernen müssen.

Themen

- Analysieren von verschachtelten Attributen
- Durchlaufen von Listen
- Verwenden von grundlegenden bedingten Anweisungen
- Erstellen von eingebetteten Teilen

Analysieren von verschachtelten Attributen

Handlebars unterstützt verschachtelte Pfade. So können Sie komplexe Benutzerdaten einfach strukturieren und in Ihren E-Mail-Vorlagen auf diese Daten verweisen.

Sie können beispielsweise Empfängerdaten in mehrere allgemeine Kategorien unterteilen. Innerhalb der einzelnen Kategorien können Sie dann detaillierte Informationen hinzufügen. Das folgende Codebeispiel zeigt, wie diese Struktur für einen einzelnen Empfänger aussehen kann:

```
{
  "meta":{
    "userId":"51806220607"
  },
  "contact":{
    "firstName":"Anaya",
    "lastName":"Iyengar",
    "city":"Bengaluru",
    "country":"India",
    "postalCode":"560052"
  },
  "subscription":[
    {
      "interest":"Sports"
```

```
    },
    {
      "interest":"Travel"
    },
    {
      "interest":"Cooking"
    }
  ]
}
```

Um in Ihren E-Mail-Vorlagen auf verschachtelte Attribute zu verweisen, geben Sie den Namen des übergeordneten Attributs, gefolgt von einem Punkt (.), gefolgt vom Namen des Attributs an, dessen Wert Sie verwenden möchten. Wenn Sie beispielsweise die Datenstruktur aus dem vorherigen Beispiel verwenden und den Vornamen des jeweiligen Empfängers in die E-Mail-Vorlage aufnehmen möchten, muss Ihre E-Mail-Vorlage folgenden Text enthalten: `Hello {{contact.firstName}}!`.

Handlebars kann mehrfach verschachtelte Pfade analysieren. Dies ermöglicht eine flexible Gestaltung Ihrer Vorlagendaten.

Durchlaufen von Listen

Die Hilfsfunktion `each` durchläuft die Elemente in einem Array. Der folgende Code ist ein Beispiel für eine E-Mail-Vorlage, die die Hilfsfunktion `each` verwendet, um eine detaillierte Liste der Interessen jedes Empfängers zu erstellen.

```
{
  "Template": {
    "TemplateName": "Preferences",
    "SubjectPart": "Subscription Preferences for {{contact.firstName}}
 {{contact.lastName}}",
    "HtmlPart": "<h1>Your Preferences</h1>
                <p>You have indicated that you are interested in receiving
                  information about the following subjects:</p>
                <ul>
                  {{#each subscription}}
                    <li>{{interest}}</li>
                  {{/each}}
                </ul>
                <p>You can change these settings at any time by visiting
                   the <a href=https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}>
                   Preference Center</a>.</p>",
```

```
    "TextPart": "Your Preferences\n\nYou have indicated that you are interested in
                receiving information about the following subjects:\n
                {{#each subscription}}
                  - {{interest}}\n
                {{/each}}
                \nYou can change these settings at any time by
                visiting the Preference Center at
                https://www.example.com/prefererences/i.aspx?id={{meta.userId}}"
  }
}
```

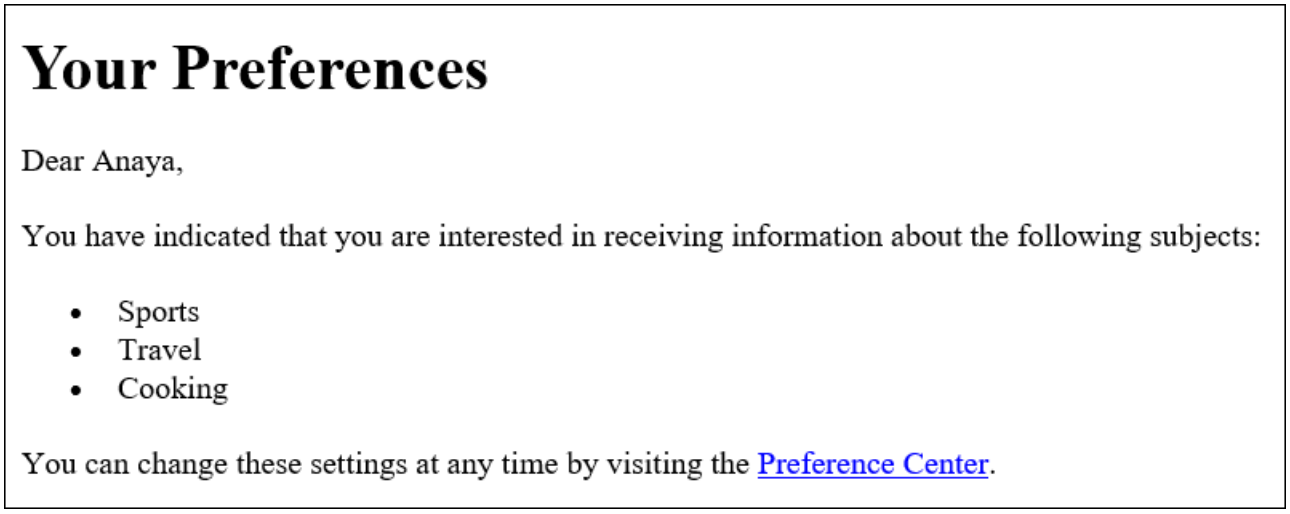
> **Important**
>
> Die Werte der Attribute `HtmlPart` und `TextPart` im vorherigen Codebeispiel enthalten Zeilenumbrüche für eine bessere Lesbarkeit. Die JSON-Datei für Ihre Vorlage darf innerhalb dieser Wert keine Zeilenumbrüche enthalten. Wenn Sie dieses Beispiel in eine eigene JSON-Datei kopiert haben, entfernen Sie die Zeilenumbrüche und zusätzlichen Leerzeichen aus den Abschnitten `HtmlPart` und `TextPart`, bevor Sie fortfahren.

Nach dem Erstellen der Vorlage können Sie die Operationen `SendEmail` oder `SendBulkEmail` verwenden, um mithilfe dieser Vorlage E-Mails an Empfänger zu senden. Sofern jeder Empfänger über mindestens einen Wert im Objekt `Interests` verfügt, erhält er eine E-Mail mit einer detaillierten Liste seiner Interessen. Das folgende Beispiel zeigt eine JSON-Datei, mit der Sie unter Verwendung der vorherigen Vorlage E-Mails an mehrere Empfänger senden können:

```
{
  "Source":"Sender Name <sender@example.com>",
  "Template":"Preferences",
  "Destinations":[
    {
      "Destination":{
        "ToAddresses":[
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementTemplateData":"{\"meta\":{\"userId\":\"51806220607\"},\"contact\":
{\"firstName\":\"Anaya\",\"lastName\":\"Iyengar\"},\"subscription\":[{\"interest\":
\"Sports\"},{\"interest\":\"Travel\"},{\"interest\":\"Cooking\"}]}"
      },
    {
```

```
      "Destination":{
        "ToAddresses":[
          "shirley.rodriguez@example.com"
        ]
      },
      "ReplacementTemplateData":"{\"meta\":{\"userId\":\"1981624758263\"},\"contact\":
{\"firstName\":\"Shirley\",\"lastName\":\"Rodriguez\"},\"subscription\":[{\"interest\":
\"Technology\"},{\"interest\":\"Politics\"}]}"
    }
  ],
  "DefaultTemplateData":"{\"meta\":{\"userId\":\"\"},\"contact\":{\"firstName\":
\"Friend\",\"lastName\":\"\"},\"subscription\":[]}"
}
```

Wenn Sie mithilfe der Operation `SendBulkEmail` eine E-Mail an die Empfänger aus dem vorherigen Beispiel senden, erhalten diese eine Nachricht ähnlich wie in der folgenden Abbildung:



Your Preferences

Dear Anaya,

You have indicated that you are interested in receiving information about the following subjects:

- Sports
- Travel
- Cooking

You can change these settings at any time by visiting the Preference Center.

Verwenden von grundlegenden bedingten Anweisungen

Dieser Abschnitt baut auf dem Beispiel aus dem vorherigen Abschnitt auf. Im Beispiel aus dem vorherigen Abschnitt wird das Hilfsprogramm `each` verwendet, um eine Liste von Interessen zu durchlaufen. Die Empfänger, für die keine Interessen hinterlegt sind, erhalten jedoch eine E-Mail mit einer leeren Liste. Wenn Sie das Hilfsprogramm `{{if}}` verwenden, können Sie die E-Mail abhängig davon, ob ein bestimmtes Attribut in den Vorlagendaten vorhanden ist, unterschiedlich formatieren. Im folgenden Code wird das Hilfsprogramm `{{if}}` verwendet, um die Liste aus dem vorherigen Abschnitt anzuzeigen, wenn das Array `Subscription` mindestens einen Wert enthält. Falls das Array leer ist, wird ein anderer Textblock angezeigt.

```
{
```

```
  "Template": {
    "TemplateName": "Preferences2",
    "SubjectPart": "Subscription Preferences for {{contact.firstName}}
 {{contact.lastName}}",
    "HtmlPart": "<h1>Your Preferences</h1>
                <p>Dear {{contact.firstName}},</p>
                {{#if subscription}}
                  <p>You have indicated that you are interested in receiving
                    information about the following subjects:</p>
                    <ul>
                    {{#each subscription}}
                      <li>{{interest}}</li>
                    {{/each}}
                    </ul>
                    <p>You can change these settings at any time by visiting
                      the <a href=https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}>
                      Preference Center</a>.</p>
                {{else}}
                  <p>Please update your subscription preferences by visiting
                    the <a href=https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}>
                    Preference Center</a>.
                {{/if}}",
    "TextPart": "Your Preferences\n\nDear {{contact.firstName}},\n\n
                {{#if subscription}}
                  You have indicated that you are interested in receiving
                  information about the following subjects:\n
                  {{#each subscription}}
                    - {{interest}}\n
                  {{/each}}
                  \nYou can change these settings at any time by visiting the
                  Preference Center at https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}.
                {{else}}
                  Please update your subscription preferences by visiting the
                  Preference Center at https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}.
                {{/if}}"
  }
}
```

> **Important**
>
> Die Werte der Attribute `HtmlPart` und `TextPart` im vorherigen Codebeispiel enthalten Zeilenumbrüche für eine bessere Lesbarkeit. Die JSON-Datei für Ihre Vorlage darf innerhalb dieser Wert keine Zeilenumbrüche enthalten. Wenn Sie dieses Beispiel in eine eigene JSON-Datei kopiert haben, entfernen Sie die Zeilenumbrüche und zusätzlichen Leerzeichen aus den Abschnitten `HtmlPart` und `TextPart`, bevor Sie fortfahren.

Das folgende Beispiel zeigt eine JSON-Datei, mit der Sie unter Verwendung der vorherigen Vorlage E-Mails an mehrere Empfänger senden können:

```
{
  "Source":"Sender Name <sender@example.com>",
  "Template":"Preferences2",
  "Destinations":[
    {
      "Destination":{
        "ToAddresses":[
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementTemplateData":"{\"meta\":{\"userId\":\"51806220607\"},\"contact\":
{\"firstName\":\"Anaya\",\"lastName\":\"Iyengar\"},\"subscription\":[{\"interest\":
\"Sports\"},{\"interest\":\"Cooking\"}]}"
      },
    {
      "Destination":{
        "ToAddresses":[
          "shirley.rodriguez@example.com"
        ]
      },
      "ReplacementTemplateData":"{\"meta\":{\"userId\":\"1981624758263\"},\"contact\":
{\"firstName\":\"Shirley\",\"lastName\":\"Rodriguez\"}}"
    }
  ],
  "DefaultTemplateData":"{\"meta\":{\"userId\":\"\"},\"contact\":{\"firstName\":
\"Friend\",\"lastName\":\"\"},\"subscription\":[]}"
}
```

In diesem Beispiel erhalten Empfänger, deren Vorlagendaten eine Liste mit Interessen enthalten, dieselbe E-Mail wie im Beispiel aus dem vorherigen Abschnitt. Empfänger, deren Vorlagendaten keine Interessen enthalten, erhalten jedoch eine E-Mail ähnlich wie in der folgenden Abbildung gezeigt:

Erstellen von eingebetteten Teilen

Mithilfe von eingebetteten Teilen können Sie Vorlagen vereinfachen, die wiederholte Zeichenfolgen enthalten. Sie können beispielweise einen eingebetteten Teil erstellen, der den Vornamen und, falls verfügbar, den Nachnamen des Empfängers enthält, Verwenden Sie dazu am Anfang Ihrer Vorlage den folgenden Code:

```
{{#* inline \"fullName\"}}{{firstName}}{{#if lastName}} {{lastName}}{{/if}}{{/
inline}}\n
```

> **Note**
>
> Das Zeilenumbruchzeichen (\n) ist erforderlich, um den `{{inline}}`-Block vom Inhalt Ihrer Vorlage zu trennen. Der Zeilenumbruch wird in der endgültigen Ausgabe nicht dargestellt.

Nachdem Sie den Teil `fullName` erstellt haben, können Sie ihn an jeder Stelle in Ihrer Vorlage verwenden, indem Sie dem Namen des Teils ein Größerzeichen (**>**) gefolgt von einem Leerzeichen voranstellen, wie im folgenden Beispiel: `{{> fullName}}`. Eingebettete Teile werden nicht zwischen den einzelnen Bestandteilen der E-Mail übertragen. Wenn Sie beispielsweise denselben eingebetteten Teil sowohl in der HTML- als auch in der Textversion der E-Mail verwenden möchten, müssen Sie ihn sowohl im Bereich `HtmlPart` als auch im Bereich `TextPart` definieren.

Sie können eingebettete Teile auch beim Durchlaufen von Arrays verwenden. Mit dem folgenden Code können Sie eine Vorlage mit dem eingebetteten Teil `fullName` erstellen. In diesem Beispiel wird der eingebettete Teil sowohl auf den Empfängernamen als auch auf ein Array mit anderen Namen angewendet:

```
{
  "Template": {
    "TemplateName": "Preferences3",
    "SubjectPart": "{{firstName}}'s Subscription Preferences",
    "HtmlPart": "{{#* inline \"fullName\"}}
                  {{firstName}}{{#if lastName}} {{lastName}}{{/if}}
                {{/inline~}}\n
                <h1>Hello {{> fullName}}!</h1>
                <p>You have listed the following people as your friends:</p>
                <ul>
                {{#each friends}}
                  <li>{{> fullName}}</li>
                {{/each}}</ul>",
    "TextPart": "{{#* inline \"fullName\"}}
                  {{firstName}}{{#if lastName}} {{lastName}}{{/if}}
                {{/inline~}}\n
                Hello {{> fullName}}! You have listed the following people
                as your friends:\n
                {{#each friends}}
                  - {{> fullName}}\n
                {{/each}}"
  }
}
```

Important

Die Werte der Attribute `HtmlPart` und `TextPart` im vorherigen Codebeispiel enthalten Zeilenumbrüche für eine bessere Lesbarkeit. Die JSON-Datei für Ihre Vorlage darf innerhalb dieser Wert keine Zeilenumbrüche enthalten. Wenn Sie dieses Beispiel in eine eigene JSON-Datei kopiert haben, entfernen Sie die Zeilenumbrüche und zusätzlichen Leerzeichen aus diesen Abschnitten.

E-Mail-Vorlagen verwalten

Neben der Erstellung von E-Mail-Vorlagen können Sie auch die Amazon SES v2-API verwenden, um bestehende Vorlagen zu aktualisieren oder zu löschen, alle Ihre vorhandenen Vorlagen aufzulisten oder den Inhalt einer Vorlage anzuzeigen.

Dieser Abschnitt enthält Verfahren zur Verwendung von AWS CLI zur Ausführung von Aufgaben im Zusammenhang mit SES-Vorlagen.

> **Note**
>
> Bei diesen Verfahren wird vorausgesetzt, dass Sie die AWS CLI bereits installiert und konfiguriert haben. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Anzeigen einer Liste von E-Mail-Vorlagen

Sie können den `ListEmailTemplate`SES v2-API-Vorgang verwenden, um eine Liste all Ihrer vorhandenen E-Mail-Vorlagen anzuzeigen.

So zeigen Sie eine Liste von E-Mail-Vorlagen an

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws sesv2 list-email-templates
  ```

  Wenn in Ihrem SES-Konto in der aktuellen Region E-Mail-Vorlagen vorhanden sind, gibt dieser Befehl eine Antwort zurück, die dem folgenden Beispiel ähnelt:

  ```
  {
      "TemplatesMetadata": [
          {
              "Name": "SpecialOffers",
              "CreatedTimestamp": "2020-08-05T16:04:12.640Z"
          },
          {
              "Name": "NewsAndUpdates",
              "CreatedTimestamp": "2019-10-03T20:03:34.574Z"
          }
      ]
  }
  ```

  Wenn Sie keine Vorlagen erstellt haben, gibt der Befehl ein `TemplatesMetadata`-Objekt ohne Member zurück.

Anzeigen des Inhalts einer bestimmten E-Mail-Vorlage

Sie können den `GetEmailTemplate`SES-v2-API-Vorgang verwenden, um den Inhalt einer bestimmten E-Mail-Vorlage anzuzeigen.

So zeigen Sie den Inhalt einer E-Mail-Vorlage an

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws sesv2 get-email-template --template-name MyTemplate
  ```

  Ersetzen Sie ihn im vorherigen Befehl *`MyTemplate`* durch den Namen der Vorlage, die Sie anzeigen möchten.

  Wenn der von Ihnen angegebene Vorlagenname mit einer Vorlage übereinstimmt, die in Ihrem SES-Konto vorhanden ist, gibt dieser Befehl eine Antwort zurück, die dem folgenden Beispiel ähnelt:

  ```
  {
      "Template": {
          "TemplateName": "TestMessage",
          "SubjectPart": "Amazon SES Test Message",
          "TextPart": "Hello! This is the text part of the message.",
          "HtmlPart": "<html>\n<body>\n<h2>Hello!</h2>\n<p>This is the HTML part of
   the message.</p></body>\n</html>"
      }
  }
  ```

  Wenn der von Ihnen angegebene Vorlagenname nicht mit einer Vorlage übereinstimmt, die in Ihrem SES-Konto vorhanden ist, gibt der Befehl einen `NotFoundException` Fehler zurück.

Löschen einer E-Mail-Vorlage

Sie können den `DeleteEmailTemplate`SES-v2-API-Vorgang verwenden, um eine bestimmte E-Mail-Vorlage zu löschen.

Löschen einer E-Mail-Vorlage

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 delete-email-template --template-name MyTemplate
```

Ersetzen Sie es im vorherigen Befehl *MyTemplate* durch den Namen der Vorlage, die Sie löschen möchten.

Dieser Befehl liefert keine Ausgabe. Mithilfe des GetTemplateVorgangs können Sie überprüfen, ob die Vorlage gelöscht wurde.

Aktualisieren einer E-Mail-Vorlage

Sie können den `UpdateEmailTemplate`SES v2-API-Vorgang verwenden, um eine vorhandene E-Mail-Vorlage zu aktualisieren. Dieser Vorgang ist beispielsweise hilfreich, wenn Sie die Betreffzeile der E-Mail-Vorlage ändern möchten oder wenn Sie den Nachrichtentext selbst ändern müssen.

Aktualisieren einer E-Mail-Vorlage

1. Verwenden Sie den `GetEmailTemplate`-Befehl, um die vorhandene Vorlage abzurufen, indem Sie den folgenden Befehl in der Befehlszeile eingeben:

   ```
   aws sesv2 get-email-template --template-name MyTemplate
   ```

   Ersetzen Sie es im vorherigen Befehl *MyTemplate* durch den Namen der Vorlage, die Sie aktualisieren möchten.

   Wenn der von Ihnen angegebene Vorlagenname mit einer Vorlage übereinstimmt, die in Ihrem SES-Konto vorhanden ist, gibt dieser Befehl eine Antwort zurück, die dem folgenden Beispiel ähnelt:

   ```
   {
       "Template": {
           "TemplateName": "TestMessage",
           "SubjectPart": "Amazon SES Test Message",
           "TextPart": "Hello! This is the text part of the message.",
           "HtmlPart": "<html>\n<body>\n<h2>Hello!</h2>\n<p>This is the HTML part of
    the message.</p></body>\n</html>"
       }
   }
   ```

2. Erstellen Sie in einem Texteditor eine neue Datei. Fügen Sie die Ausgabe des vorherigen Befehls in die Datei ein.
3. Ändern Sie die Vorlage nach Bedarf. Alle Zeilen, die Sie auslassen, werden aus der Vorlage entfernt. Wenn Sie beispielsweise nur `SubjectPart` der Vorlage ändern möchten, müssen Sie dennoch die `TextPart` und `HtmlPart`-Eigenschaften einschließen.

   Wenn Sie fertig sind, speichern Sie die Datei unter `update_template.json`.
4. Geben Sie in der Befehlszeile folgenden Befehl ein:

   ```
   aws sesv2 update-email-template --cli-input-json file://path/to/
   update_template.json
   ```

   Ersetzen Sie im vorherigen Befehl *`path/to/update_template.json`* durch den Pfad zu der `update_template.json` Datei, die Sie im vorherigen Schritt erstellt haben.

   Wenn die Vorlage erfolgreich aktualisiert wurde, liefert dieser Befehl keine Ausgabe. Mithilfe des `GetEmailTemplate`Vorgangs können Sie überprüfen, ob die Vorlage aktualisiert wurde.

   Wenn die angegebene Vorlage nicht vorhanden ist, gibt dieser Befehl einen `TemplateDoesNotExist`-Fehler zurück. Wenn die Vorlage weder die Eigenschaft `TextPart` oder `HtmlPart` (weder beides) enthält, gibt dieser Befehl einen `InvalidParameterValue`-Fehler zurück.

Senden von E-Mails über Amazon SES mithilfe eines AWS SDK

Sie können ein AWS SDK verwenden, um E-Mails über Amazon SES zu versenden. AWS SDKs sind für mehrere Programmiersprachen verfügbar. Weitere Informationen finden Sie unter Tools für Amazon Web Services.

Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein, um die Codebeispiele im nächsten Abschnitt auszufüllen:

- Sofern noch nicht geschehen, führen die Schritte unter au Amazon Simple Email Service einrichten.
- Verifizieren Sie Ihre E-Mail-Adresse mit Amazon SES – Bevor Sie E-Mails mit &SES; senden können, müssen Sie den Besitz der Absender-E-Mail-Adresse nachweisen. Befindet sich Ihr

Konto noch in der Amazon SES Sandbox, müssen Sie auch die E-Mail-Adresse des Empfängers verifizieren. Wir empfehlen Ihnen, die Amazon SES Konsole zu verwenden, um E-Mail-Adressen zu verifizieren. Weitere Informationen finden Sie unter Erstellen einer E-Mail-Adressidentität.

- Holen Sie sich Ihre AWS Anmeldeinformationen — Sie benötigen eine AWS Zugriffsschlüssel-ID und einen AWS geheimen Zugriffsschlüssel, um mit einem SDK auf Amazon SES zuzugreifen. Sie erhalten Ihre Anmeldeinformationen über die Seite Security Credentials (Sicherheitsanmeldeinformationen) in der AWS-Managementkonsole. Weitere Informationen zu Anmeldeinformationen finden Sie unter Arten von Amazon-SES-Anmeldeinformationen.
- Erstellen einer gemeinsamen Anmeldeinformationsdatei – Damit der Beispiel-Code in diesem Abschnitt ordnungsgemäß funktioniert, müssen Sie eine gemeinsame Anmeldeinformationsdatei erstellen. Weitere Informationen finden Sie unter Erstellen einer gemeinsamen Anmeldeinformationsdatei zur Verwendung beim Senden von E-Mails über Amazon SES mithilfe eines AWS SDK.

Codebeispiele

> **Important**
>
> In diesem Tutorial senden Sie eine E-Mail an sich selbst, um zu prüfen, ob diese bei Ihnen ankommt. Für weitere Experimente oder Lasttests nutzen Sie den Amazon SES-Postfachsimulator. E-Mails, die Sie an den Postfachsimulator senden, zählen nicht zu Ihrer Sendequote oder Ihre Unzustellbarkeits- und Beschwerderate. Weitere Informationen finden Sie unter Manuelles Verwenden des Postfachsimulators.

.NET

Im folgenden Verfahren wird beschrieben, wie Sie mit Amazon SES eine E-Mail über Visual Studio und AWS SDK für .NET senden.

Diese Lösung wurde mit folgenden Komponenten getestet:

- Microsoft Visual Studio Community 2017, Version 15.4.0.
- Microsoft .NET Framework, Version 4.6.1.
- Das AWSSDK .Core-Paket (Version 3.3.19), installiert mit. NuGet
- AWSSDKDas. SimpleEmail Paket (Version 3.3.6.1), installiert mit. NuGet

Führen Sie vor Beginn die folgenden Schritte durch:

- Visual Studio installieren — Visual Studio ist unter/verfügbar. https://www.visualstudio.com

Um eine E-Mail mit dem zu senden AWS SDK für .NET

1. Führen Sie die folgenden Schritte aus, um ein neues Projekt zu erstellen:
   a. Starten Sie Visual Studio.
   b. Wählen Sie im Menü File (Datei) New (Neu), Project (Projekt) aus.
   c. Erweitern Sie im linken Bereich des Fensters New Project (Neues Projekt) die Einträge Installed (Installiert) und Visual C#.
   d. Wählen Sie im rechten Bereich Konsolen-App (.NET Framework) aus.
   e. Geben Sie unter Name **`AmazonSESSample`** ein und klicken Sie auf OK.
2. Verwenden Sie diese Option NuGet , um die Amazon SES SES-Pakete in Ihre Lösung aufzunehmen, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im Solution Explorer-Bereich mit der rechten Maustaste auf Ihr Projekt und wählen Sie dann NuGet Pakete verwalten.
   b. Wählen Sie auf der SESSample Registerkarte NuGet: Amazon die Option Durchsuchen aus.
   c. Geben Sie in das Suchfeld **`AWSSDK.SimpleEmail`** ein.
   d. Wählen Sie die AWSSDK. SimpleEmailPaket und wählen Sie dann Installieren.
   e. Klicken Sie im Fenster Preview Changes (Vorschau der Änderungen) auf OK.
3. Fügen Sie auf der Registerkarte Program.cs folgenden Code hinzu:

```
using Amazon;
using System;
using System.Collections.Generic;
using Amazon.SimpleEmail;
using Amazon.SimpleEmail.Model;

namespace AmazonSESSample
{
    class Program
    {
        // Replace sender@example.com with your "From" address.
```

```
        // This address must be verified with Amazon SES.
        static readonly string senderAddress = "sender@example.com";

        // Replace recipient@example.com with a "To" address. If your account
        // is still in the sandbox, this address must be verified.
        static readonly string receiverAddress = "recipient@example.com";

        // The configuration set to use for this email. If you do not want to
 use a
        // configuration set, comment out the following property and the
        // ConfigurationSetName = configSet argument below.
        static readonly string configSet = "ConfigSet";

        // The subject line for the email.
        static readonly string subject = "Amazon SES test (AWS SDK für .NET)";

        // The email body for recipients with non-HTML email clients.
        static readonly string textBody = "Amazon SES Test (.NET)\r\n"
                                        + "This email was sent through Amazon
 SES "
                                        + "using the AWS SDK für .NET.";

        // The HTML body of the email.
        static readonly string htmlBody = @"<html>
<head></head>
<body>
  <h1>Amazon SES Test (SDK für .NET)</h1>
  <p>This email was sent with
    <a href='https://aws.amazon.com/ses/'>Amazon SES</a> using the
    <a href='https://aws.amazon.com/sdk-for-net/'> AWS SDK für .NET</a>.</p>
</body>
</html>";

        static void Main(string[] args)
        {
            // Replace USWest2 with the AWS Region you're using for Amazon SES.
            // Acceptable values are EUWest1, USEast1, and USWest2.
            using (var client = new
 AmazonSimpleEmailServiceClient(RegionEndpoint.USWest2))
            {
                var sendRequest = new SendEmailRequest
                {
                    Source = senderAddress,
                    Destination = new Destination
```

```
                    {
                        ToAddresses =
                        new List<string> { receiverAddress }
                    },
                    Message = new Message
                    {
                        Subject = new Content(subject),
                        Body = new Body
                        {
                            Html = new Content
                            {
                                Charset = "UTF-8",
                                Data = htmlBody
                            },
                            Text = new Content
                            {
                                Charset = "UTF-8",
                                Data = textBody
                            }
                        }
                    },
                    // If you are not using a configuration set, comment
                    // or remove the following line
                    ConfigurationSetName = configSet
                };
                try
                {
                    Console.WriteLine("Sending email using Amazon SES...");
                    var response = client.SendEmail(sendRequest);
                    Console.WriteLine("The email was sent successfully.");
                }
                catch (Exception ex)
                {
                    Console.WriteLine("The email was not sent.");
                    Console.WriteLine("Error message: " + ex.Message);

                }
            }

            Console.Write("Press any key to continue...");
            Console.ReadKey();
        }
    }
```

```
}
```

4. Führen Sie im Code-Editor die folgenden Schritte aus:

   - *sender@example.com*Ersetzen Sie es durch die E-Mail-Adresse „Von:“. Diese Adresse muss verifiziert werden. Weitere Informationen finden Sie unter Verifizierte Identitäten.
   - *recipient@example.com*Ersetzen Sie es durch die Adresse „An:“. Wenn sich Ihr Konto noch in der Sandbox befindet, muss auch diese Adresse verifiziert werden.
   - *ConfigSet*Ersetzen Sie es durch den Namen des Konfigurationssatzes, der beim Senden dieser E-Mail verwendet werden soll.
   - *USWest2*Ersetzen Sie es durch den Namen des AWS-Region Endpunkts, den Sie zum Senden von E-Mails mit Amazon SES verwenden. Eine Liste der Regionen, in denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.

   Wenn Sie fertig sind, speichern Sie `Program.cs`.
5. Führen Sie die folgenden Schritte durch, um die Anwendung zu erstellen und auszuführen:

   a. Wählen Sie im Menü Build (Erstellen) Build Solution (Lösung erstellen) aus.

   b. Klicken Sie im Menü Debug (Debuggen) auf Start Debugging (Debuggen starten). Ein Konsolenfenster wird angezeigt.
6. Überprüfen Sie die Ausgabe der Konsole. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole „`The email was sent successfully.`“.
7. Wenn die E-Mail erfolgreich übermittelt wurde, melden Sie sich beim E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

Java

Das folgende Verfahren zeigt Ihnen, wie Sie Eclipse IDE für Java EE-Entwickler verwenden und AWS Toolkit for Eclipseein AWS SDK-Projekt erstellen und den Java-Code ändern, um eine E-Mail über Amazon SES zu senden.

Führen Sie vor Beginn die folgenden Schritte durch:

- Eclipse installieren – Sie können Eclipse unter https://www.eclipse.org/downloads herunterladen. Der Code in diesem Tutorial wurde mit Eclipse Neon.3 (Version 4.6.3) und Version 1.8 der Java Runtime Environment geprüft.

- Installieren Sie das AWS Toolkit for Eclipse — Anweisungen zum Hinzufügen von AWS Toolkit for Eclipse zu Ihrer Eclipse-Installation finden Sie unter https://aws.amazon.com/eclipse. Der Code in diesem Tutorial wurde unter Verwendung der Version 2.3.1 des AWS Toolkit for Eclipse getestet.

Um eine E-Mail mit dem zu senden AWS SDK für Java

1. Erstellen Sie ein AWS Java-Projekt in Eclipse, indem Sie die folgenden Schritte ausführen:
   a. Starten Sie Eclipse.
   b. Wählen Sie im Menü File (Datei) die Option New (Neu) und wählen Sie dann Other (Weitere) aus. Erweitern Sie im Fenster New (Neu) den Ordner AWS und wählen Sie dann AWS Java Project (Java-Projekt) aus.
   c. Gehen Sie im Dialogfeld „Neues AWS Java-Projekt“ wie folgt vor:
      i. Geben Sie im Feld Project name (Projektname) einen Namen für das Projekt ein.
      ii. Wählen Sie unter AWS SDK für Java Beispiele die Option Amazon Simple Email Service JavaMail Sample aus.
      iii. Klicken Sie auf Finish (Abschließen).
2. Erweitern Sie im Bereich Package Explorer (Paket-Explorer) das Projekt.
3. Erweitern Sie im `src/main/java`-Ordner den `com.amazon.aws.samples`-Ordner und klicken Sie doppelt auf `AmazonSESSample.java`.
4. Ersetzen Sie den gesamten Inhalt von `AmazonSESSample.java` durch den folgenden Code:

```
package com.amazonaws.samples;

import java.io.IOException;

import com.amazonaws.regions.Regions;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailService;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailServiceClientBuilder;
import com.amazonaws.services.simpleemail.model.Body;
import com.amazonaws.services.simpleemail.model.Content;
import com.amazonaws.services.simpleemail.model.Destination;
import com.amazonaws.services.simpleemail.model.Message;
import com.amazonaws.services.simpleemail.model.SendEmailRequest;

public class AmazonSESSample {
```

```
  // Replace sender@example.com with your "From" address.
  // This address must be verified with Amazon SES.
  static final String FROM = "sender@example.com";

  // Replace recipient@example.com with a "To" address. If your account
  // is still in the sandbox, this address must be verified.
  static final String TO = "recipient@example.com";

  // The configuration set to use for this email. If you do not want to use a
  // configuration set, comment the following variable and the
  // .withConfigurationSetName(CONFIGSET); argument below.
  static final String CONFIGSET = "ConfigSet";

  // The subject line for the email.
  static final String SUBJECT = "Amazon SES test (AWS SDK für Java)";

  // The HTML body for the email.
  static final String HTMLBODY = "<h1>Amazon SES test (AWS SDK für Java)</h1>"
      + "<p>This email was sent with <a href='https://aws.amazon.com/ses/'>"
      + "Amazon SES</a> using the <a href='https://aws.amazon.com/sdk-for-
java/'>"
      + "AWS SDK for Java</a>";

  // The email body for recipients with non-HTML email clients.
  static final String TEXTBODY = "This email was sent through Amazon SES "
      + "using the AWS SDK für Java.";

  public static void main(String[] args) throws IOException {

    try {
      AmazonSimpleEmailService client =
          AmazonSimpleEmailServiceClientBuilder.standard()
          // Replace US_WEST_2 with the AWS Region you're using for
          // Amazon SES.
            .withRegion(Regions.US_WEST_2).build();
      SendEmailRequest request = new SendEmailRequest()
          .withDestination(
              new Destination().withToAddresses(TO))
          .withMessage(new Message()
              .withBody(new Body()
                  .withHtml(new Content()
                      .withCharset("UTF-8").withData(HTMLBODY))
                  .withText(new Content()
```

```
                        .withCharset("UTF-8").withData(TEXTBODY)))
                .withSubject(new Content()
                    .withCharset("UTF-8").withData(SUBJECT)))
            .withSource(FROM)
            // Comment or remove the next line if you are not using a
            // configuration set
            .withConfigurationSetName(CONFIGSET);
        client.sendEmail(request);
        System.out.println("Email sent!");
      } catch (Exception ex) {
        System.out.println("The email was not sent. Error message: "
            + ex.getMessage());
      }
    }
}
```

5. Ersetzen Sie in `AmazonSESSample.java` folgende Werte durch Ihre eigenen Werte:

> **Important**
>
> Bei den E-Mail-Adressen ist die Groß-/Kleinschreibung nicht relevant. Vergewissern Sie sich, dass die Adressen exakt mit denen übereinstimmen, die Sie verifiziert haben.

   - `SENDER@EXAMPLE.COM` – Ersetzen Sie dies durch Ihre Absender-E-Mail-Adresse. Sie müssen diese Adresse verifizieren, bevor Sie das Programm ausführen. Weitere Informationen finden Sie unter Verifizierte Identitäten in Amazon SES.
   - `RECIPIENT@EXAMPLE.COM` – Ersetzen Sie dies durch die Empfänger-E-Mail-Adresse. Wenn sich Ihr Konto noch in der Sandbox befindet, müssen Sie diese Adresse verifizieren, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).
   - (Optional) **`us-west-2`** – Wenn Amazon SES in einer anderen Region als USA West (Oregon) verwendet werden soll, ersetzen Sie dies durch die entsprechende Region. Eine Liste der Regionen, in denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.
6. Speichern `AmazonSESSample.java`.
7. Wählen Sie Project (Projekt) und dann Build Project (Projekt entwickeln) aus.

> **Note**
>
> Wenn diese Option deaktiviert ist, kann die automatische Erstellung aktiviert sein. Wenn dies der Fall ist, können Sie diesen Schritt überspringen.

8. Wählen Sie Run (Ausführen) und dann erneut Run (Ausführen) aus, um das Programm zu starten und die E-Mail zu senden.
9. Sehen Sie sich die Ausgabe im Konsolenbereich in Eclipse an. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole „`Email sent!`“ an. Andernfalls wird eine Fehlermeldung angezeigt.
10. Wenn die E-Mail erfolgreich übermittelt wurde, melden Sie sich beim E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

PHP

In diesem Thema erfahren Sie, wie Sie das AWS SDK für PHP verwenden, um eine E-Mail über Amazon SES zu senden.

Führen Sie vor Beginn die folgenden Schritte durch:

- Installieren von PHP – PHP finden Sie unter http://php.net/downloads.php. Für dieses Tutorial ist die PHP-Version 5.5 oder höher erforderlich. Fügen Sie nach der Installation von PHP Ihren Umgebungsvariablen den Pfad zu PHP hinzu, damit Sie PHP von jeder Eingabeaufforderung aus ausführen können. Der Code in diesem Tutorial wurde unter Verwendung von PHP 7.2.7 getestet.
- AWS SDK für PHP Version 3 installieren — Anweisungen zum Herunterladen und zur Installation finden Sie in der AWS SDK für PHP Dokumentation. Der Code in diesem Tutorial wurde unter Verwendung der Version 3.64.13 des SDKs getestet.

Um eine E-Mail über Amazon SES zu senden, verwenden Sie AWS SDK für PHP

1. Erstellen Sie in einem Texteditor eine Datei mit dem Namen `amazon-ses-sample.php`. Fügen Sie folgenden Code ein:

```
<?php

// If necessary, modify the path in the require statement below to refer to the
```

```
// location of your Composer autoload.php file.
require 'vendor/autoload.php';

use Aws\Ses\SesClient;
use Aws\Exception\AwsException;

// Create an SesClient. Change the value of the region parameter if you're
// using an AWS Region other than US West (Oregon). Change the value of the
// profile parameter if you want to use a profile in your credentials file
// other than the default.
$SesClient = new SesClient([
    'profile' => 'default',
    'version' => '2010-12-01',
    'region'  => 'us-west-2'
]);

// Replace sender@example.com with your "From" address.
// This address must be verified with Amazon SES.
$sender_email = 'sender@example.com';

// Replace these sample addresses with the addresses of your recipients. If
// your account is still in the sandbox, these addresses must be verified.
$recipient_emails = ['recipient1@example.com','recipient2@example.com'];

// Specify a configuration set. If you do not want to use a configuration
// set, comment the following variable, and the
// 'ConfigurationSetName' => $configuration_set argument below.
$configuration_set = 'ConfigSet';

$subject = 'Amazon SES test (AWS SDK für PHP)';
$plaintext_body = 'This email was sent with Amazon SES using the AWS SDK for
 PHP.' ;
$html_body =  '<h1>AWS Amazon Simple Email Service Test Email</h1>'.
              '<p>This email was sent with <a href="https://aws.amazon.com/
ses/">'.
              'Amazon SES</a> using the <a href="https://aws.amazon.com/sdk-for-
php/">'.
              'AWS SDK für PHP</a>.</p>';
$char_set = 'UTF-8';

try {
    $result = $SesClient->sendEmail([
        'Destination' => [
            'ToAddresses' => $recipient_emails,
```

```
        ],
        'ReplyToAddresses' => [$sender_email],
        'Source' => $sender_email,
        'Message' => [
          'Body' => [
              'Html' => [
                  'Charset' => $char_set,
                  'Data' => $html_body,
              ],
              'Text' => [
                  'Charset' => $char_set,
                  'Data' => $plaintext_body,
              ],
          ],
          'Subject' => [
              'Charset' => $char_set,
              'Data' => $subject,
          ],
        ],
        // If you aren't using a configuration set, comment or delete the
        // following line
        'ConfigurationSetName' => $configuration_set,
    ]);
    $messageId = $result['MessageId'];
    echo("Email sent! Message ID: $messageId"."\n");
} catch (AwsException $e) {
    // output error message if fails
    echo $e->getMessage();
    echo("The email was not sent. Error message: ".$e-
>getAwsErrorMessage()."\n");
    echo "\n";
}
```

2. Ersetzen Sie in `amazon-ses-sample.php` folgende Werte durch Ihre eigenen Werte:

   - **`path_to_sdk_inclusion`**— Ersetzt durch den Pfad, der erforderlich ist, um das AWS SDK für PHP in das Programm aufzunehmen. Weitere Informationen finden Sie in der AWS SDK für PHP -Dokumentation.
   - **`sender@example.com`** – Ersetzen Sie dies durch eine E-Mail-Adresse, die für Amazon SES verifiziert wurde. Weitere Informationen finden Sie unter Verifizierte Identitäten. Bei den E-Mail-Adressen in Amazon SES wird die Groß-/Kleinschreibung beachtet. Stellen

Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.

- **`recipient1@example.com`**, **`recipient2@example.com`** – ersetzen Sie dies durch Ihre Empfängeradressen. Wenn sich Ihr Konto noch in der Sandbox befindet, muss auch die Empfängeradresse verifiziert werden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox). Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
- (Optional) **`ConfigSet`**—Wenn Sie beim Senden dieser E-Mail einen Konfigurationssatz senden möchten, ändern Sie den Wert der Variable mit dem Namen des Konfigurationssatzes. Weitere Informationen zu Konfigurationssätzen finden Sie unter Verwenden von Amazon SES-Konfigurationssätzen im.
- (Optional) **`us-west-2`** – Wenn Amazon SES in einer anderen Region als USA West (Oregon) verwendet werden soll, ersetzen Sie dies durch die entsprechende Region. Eine Liste der Regionen, in denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.

3. Speichern `amazon-ses-sample.php`.
4. Um das Programm zu starten, öffnen Sie eine Eingabeaufforderung in demselben Verzeichnis wie `amazon-ses-sample.php` und geben Sie dann den folgenden Befehl ein:

```
$ php amazon-ses-sample.php
```

5. Überprüfen Sie die Ausgabe. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole „`Email sent!`“ an. Andernfalls wird eine Fehlermeldung angezeigt.

> **Note**
>
> Wenn der Fehler „cURL error 60: SSL certificate problem“ angezeigt wird, wenn Sie das Programm ausführen, laden Sie das neueste CA-Bundle herunter, wie in der AWS SDK für PHP -Dokumentation beschrieben. Fügen Sie dann in `amazon-ses-sample.php` dem `SesClient::factory`-Array die folgenden Zeilen hinzu, ersetzen Sie `path_of_certs` durch den Pfad zu dem heruntergeladenen CA-Bundle und führen Sie das Programm erneut aus.
>
> ```
> 'http' => [
>    'verify' => 'path_of_certs\ca-bundle.crt'
> ```

```
]
```

6. Melden Sie sich am E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

Ruby

In diesem Thema erfahren Sie, wie Sie das AWS SDK für Ruby verwenden, um eine E-Mail über Amazon SES zu senden.

Führen Sie vor Beginn die folgenden Schritte durch:

- Ruby installieren — Ruby ist unter https://www.ruby-lang verfügbar. org/en/downloads/. Der Code in diesem Tutorial wurde unter Verwendung von Ruby 1.9.3 getestet. Fügen Sie nach der Installation von Ruby Ihren Umgebungsvariablen den Pfad zu Ruby hinzu, damit Sie Ruby von jeder Eingabeaufforderung aus ausführen können.
- Installieren Sie das AWS SDK für Ruby — Anweisungen zum Herunterladen und zur Installation finden Sie unter Installation von AWS SDK für Ruby im AWS SDK für Ruby Entwicklerhandbuch. Der Beispiel-Code in diesem Tutorial wurde mit Version 2.9.36 des AWS SDK für Ruby getestet.
- Erstellen einer gemeinsamen Anmeldeinformationsdatei – Damit der Beispiel-Code in diesem Abschnitt ordnungsgemäß funktioniert, müssen Sie eine gemeinsame Anmeldeinformationsdatei erstellen. Weitere Informationen finden Sie unter Erstellen einer gemeinsamen Anmeldeinformationsdatei zur Verwendung beim Senden von E-Mails über Amazon SES mithilfe eines AWS SDK.

Um eine E-Mail über Amazon SES zu senden, verwenden Sie AWS SDK für Ruby

1. Erstellen Sie in einem Texteditor eine Datei mit dem Namen `amazon-ses-sample.rb`. Fügen Sie folgenden Code in die Datei ein:

```
require 'aws-sdk'

# Replace sender@example.com with your "From" address.
# This address must be verified with Amazon SES.
sender = "sender@example.com"

# Replace recipient@example.com with a "To" address. If your account
```

```
# is still in the sandbox, this address must be verified.
recipient = "recipient@example.com"

# Specify a configuration set. If you do not want to use a configuration
# set, comment the following variable and the
# configuration_set_name: configsetname argument below.
configsetname = "ConfigSet"

# Replace us-west-2 with the AWS Region you're using for Amazon SES.
awsregion = "us-west-2"

# The subject line for the email.
subject = "Amazon SES test (AWS SDK für Ruby)"

# The HTML body of the email.
htmlbody =
  '<h1>Amazon SES test (AWS SDK für Ruby)</h1>'\
  '<p>This email was sent with <a href="https://aws.amazon.com/ses/">'\
  'Amazon SES</a> using the <a href="https://aws.amazon.com/sdk-for-ruby/">'\
  'AWS SDK für Ruby</a>.'

# The email body for recipients with non-HTML email clients.
textbody = "This email was sent with Amazon SES using the AWS SDK für Ruby."

# Specify the text encoding scheme.
encoding = "UTF-8"

# Create a new SES resource and specify a region
ses = Aws::SES::Client.new(region: awsregion)

# Try to send the email.
begin

  # Provide the contents of the email.
  resp = ses.send_email({
    destination: {
      to_addresses: [
        recipient,
      ],
    },
    message: {
      body: {
        html: {
          charset: encoding,
```

```
          data: htmlbody,
        },
        text: {
          charset: encoding,
          data: textbody,
        },
      },
      subject: {
        charset: encoding,
        data: subject,
      },
    },
  source: sender,
  # Comment or remove the following line if you are not using
  # a configuration set
  configuration_set_name: configsetname,
  })
  puts "Email sent!"

# If something goes wrong, display an error message.
rescue Aws::SES::Errors::ServiceError => error
  puts "Email not sent. Error message: #{error}"

end
```

2. Ersetzen Sie in `amazon-ses-sample.rb` folgende Werte durch Ihre eigenen Werte:

   - **`sender@example.com`** – Ersetzen Sie dies durch eine E-Mail-Adresse, die für Amazon SES verifiziert wurde. Weitere Informationen finden Sie unter Verifizierte Identitäten. Bei den E-Mail-Adressen in Amazon SES wird die Groß-/Kleinschreibung beachtet. Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
   - **`recipient@example.com`**—Ersetzen Sie dies durch die Empfängeradresse. Wenn sich Ihr Konto noch in der Sandbox befindet, müssen Sie diese Adresse verifizieren, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox). Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
   - (Optional) **`us-west-2`** – Wenn Amazon SES in einer anderen Region als USA West (Oregon) verwendet werden soll, ersetzen Sie dies durch die entsprechende Region. Eine Liste der Regionen, in denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.

3. Speichern `amazon-ses-sample.rb`.
4. Um das Programm zu starten, öffnen Sie eine Eingabeaufforderung in demselben Verzeichnis wie `amazon-ses-sample.rb` und geben Sie ruby amazon-ses-sample.rb ein.
5. Überprüfen Sie die Ausgabe. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole „`Email sent!`“ an. Andernfalls wird eine Fehlermeldung angezeigt.
6. Melden Sie sich am E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

Python

In diesem Thema erfahren Sie, wie Sie das AWS SDK für Python (Boto) verwenden, um eine E-Mail über Amazon SES zu senden.

Führen Sie vor Beginn die folgenden Schritte durch:

- Verifizieren Sie Ihre E-Mail-Adresse mit Amazon SES – Bevor Sie E-Mails mit &SES; senden können, müssen Sie den Besitz der Absender-E-Mail-Adresse nachweisen. Befindet sich Ihr Konto noch in der Amazon SES Sandbox, müssen Sie auch die E-Mail-Adresse des Empfängers verifizieren. Wir empfehlen Ihnen, die Amazon SES Konsole zu verwenden, um E-Mail-Adressen zu verifizieren. Weitere Informationen finden Sie unter Erstellen einer E-Mail-Adressidentität.
- Holen Sie sich Ihre AWS Anmeldeinformationen — Sie benötigen eine AWS Zugriffsschlüssel-ID und einen AWS geheimen Zugriffsschlüssel, um mit einem SDK auf Amazon SES zuzugreifen. Sie erhalten Ihre Anmeldeinformationen über die Seite Security Credentials (Sicherheitsanmeldeinformationen) der AWS-Managementkonsole. Weitere Informationen zu Anmeldeinformationen finden Sie unter Arten von Amazon-SES-Anmeldeinformationen.
- Python installieren — Python ist unter thon.org/downloads/ https://www.py verfügbar. Der Code in diesem Tutorial wurde mit Python 2.7.6 und Python 3.6.1 getestet. Fügen Sie nach der Installation von Python Ihren Umgebungsvariablen den Pfad zu Python hinzu, damit Sie Python von jeder Eingabeaufforderung aus ausführen können.
- Installieren Sie das AWS SDK für Python (Boto)— Anweisungen zum Herunterladen und zur Installation finden Sie in der Dokumentation.AWS SDK für Python (Boto) Der Beispiel-Code in diesem Tutorial wurde mit Version 1.4.4 des SDK für Python getestet.

So senden Sie mit dem SDK für Python eine E-Mail über Amazon SES

1. Erstellen Sie in einem Texteditor eine Datei mit dem Namen `amazon-ses-sample.py`. Fügen Sie folgenden Code in die Datei ein:

```
import boto3
from botocore.exceptions import ClientError

# Replace sender@example.com with your "From" address.
# This address must be verified with Amazon SES.
SENDER = "Sender Name <sender@example.com>"

# Replace recipient@example.com with a "To" address. If your account
# is still in the sandbox, this address must be verified.
RECIPIENT = "recipient@example.com"

# Specify a configuration set. If you do not want to use a configuration
# set, comment the following variable, and the
# ConfigurationSetName=CONFIGURATION_SET argument below.
CONFIGURATION_SET = "ConfigSet"

# If necessary, replace us-west-2 with the AWS Region you're using for Amazon
 SES.
AWS_REGION = "us-west-2"

# The subject line for the email.
SUBJECT = "Amazon SES Test (SDK for Python)"

# The email body for recipients with non-HTML email clients.
BODY_TEXT = ("Amazon SES Test (Python)\r\n"
             "This email was sent with Amazon SES using the "
             "AWS SDK für Python (Boto)."
            )

# The HTML body of the email.
BODY_HTML = """<html>
<head></head>
<body>
  <h1>Amazon SES Test (SDK for Python)</h1>
  <p>This email was sent with
    <a href='https://aws.amazon.com/ses/'>Amazon SES</a> using the
    <a href='https://aws.amazon.com/sdk-for-python/'> AWS SDK für Python
 (Boto)</a>.</p>
```

```
</body>
</html>
            """

# The character encoding for the email.
CHARSET = "UTF-8"

# Create a new SES resource and specify a region.
client = boto3.client('ses',region_name=AWS_REGION)

# Try to send the email.
try:
    #Provide the contents of the email.
    response = client.send_email(
        Destination={
            'ToAddresses': [
                RECIPIENT,
            ],
        },
        Message={
            'Body': {
                'Html': {
                    'Charset': CHARSET,
                    'Data': BODY_HTML,
                },
                'Text': {
                    'Charset': CHARSET,
                    'Data': BODY_TEXT,
                },
            },
            'Subject': {
                'Charset': CHARSET,
                'Data': SUBJECT,
            },
        },
        Source=SENDER,
        # If you are not using a configuration set, comment or delete the
        # following line
        ConfigurationSetName=CONFIGURATION_SET,
    )
# Display an error if something goes wrong.
except ClientError as e:
    print(e.response['Error']['Message'])
else:
```

```
    print("Email sent! Message ID:"),
    print(response['MessageId'])
```

2. Ersetzen Sie in `amazon-ses-sample.py` folgende Werte durch Ihre eigenen Werte:

   - **`sender@example.com`** – Ersetzen Sie dies durch eine E-Mail-Adresse, die für Amazon SES verifiziert wurde. Weitere Informationen finden Sie unter Verifizierte Identitäten. Bei den E-Mail-Adressen in Amazon SES wird die Groß-/Kleinschreibung beachtet. Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
   - **`recipient@example.com`**—Ersetzen Sie dies durch die Empfängeradresse. Wenn sich Ihr Konto noch in der Sandbox befindet, müssen Sie diese Adresse verifizieren, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox). Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
   - (Optional) **`us-west-2`** – Wenn Amazon SES in einer anderen Region als USA West (Oregon) verwendet werden soll, ersetzen Sie dies durch die entsprechende Region. Eine Liste der Regionen, in denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.

3. Speichern `amazon-ses-sample.py`.
4. Um das Programm zu starten, öffnen Sie eine Eingabeaufforderung in demselben Verzeichnis wie `amazon-ses-sample.py` und geben Sie python amazon-ses-sample.py ein.
5. Überprüfen Sie die Ausgabe. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole „`Email sent!`“ an. Andernfalls wird eine Fehlermeldung angezeigt.
6. Melden Sie sich am E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

Erstellen einer gemeinsamen Anmeldeinformationsdatei zur Verwendung beim Senden von E-Mails über Amazon SES mithilfe eines AWS SDK

Anhand des folgenden Verfahrens wird gezeigt, wie eine freigegebene Anmeldeinformationsdatei in Ihrem Stammverzeichnis erstellt wird. Damit der SDK-Beispiel-Code ordnungsgemäß funktioniert, müssen Sie diese Datei erstellen.

1. Erstellen Sie in einem Texteditor eine neue Datei. Fügen Sie folgenden Code in die Datei ein:

```
[default]
aws_access_key_id = YOUR_AWS_ACCESS_KEY_ID
aws_secret_access_key = YOUR_AWS_SECRET_ACCESS_KEY
```

2. Ersetzen Sie in der Textdatei, die Sie gerade erstellt haben, `YOUR_AWS_ACCESS_KEY` durch Ihre eindeutige AWS Zugriffsschlüssel-ID und dann `YOUR_AWS_SECRET_ACCESS_KEY` durch Ihren eindeutigen AWS geheimen Zugriffsschlüssel.
3. Speichern Sie die Datei. In der folgenden Tabelle sind die richtigen Speicherorte und Dateinamen für Ihr Betriebssystem aufgeführt.

Verwendetes Betriebssystem	Speichern Sie die Datei als...
Windows	`C:\Users\<yourUserName>\.aws\credentials`
Linux, macOS oder Unix	`~/.aws/credentials`

> **Important**
>
> Geben Sie keine Dateierweiterung ein, wenn Sie die Anmeldeinformationsdatei speichern.

Von Amazon SES unterstützte Inhaltskodierungen

Die folgenden Angaben dienen als Referenz.

Amazon SES unterstützt die folgenden Inhaltskodierungen:

- `deflate`
- `gzip`
- `identity`

Darüber hinaus unterstützt Amazon SES das folgende „Accept–Enconding“-Header-Format gemäß RFC 7231-Spezifikation:

- `Accept-Encoding:deflate,gzip`
- `Accept-Encoding:`
- `Accept-Encoding:*`
- `Accept-Encoding:deflate;q=0.5,gzip;q=1.0`
- `Accept-Encoding:gzip;q=1.0,identity;q=0.5,*;q=0`

Amazon SES und Sicherheitsprotokolle

In diesem Thema werden die Sicherheitsprotokolle beschrieben, die Sie verwenden können, wenn Sie eine Verbindung mit Amazon SES herstellen, sowie wenn Amazon SES eine E-Mail an einen Empfänger übermittelt.

E-Mail-Absender an Amazon SES

Welches Sicherheitsprotokoll Sie verwenden, um eine Verbindung mit herzustellen, hängt davon ab, ob Sie die Amazon-SES-API- oder die Amazon-SES-SMTP-Schnittstelle verwenden, wie im Folgenden beschrieben.

HTTPS

Wenn Sie die Amazon SES SES-API (entweder direkt oder über ein AWS SDK) verwenden, wird die gesamte Kommunikation mit TLS über den Amazon SES SES-HTTPS-Endpunkt verschlüsselt. Der HTTPS-Endpunkt von Amazon SES unterstützt TLS 1.2 und TLS 1.3.

SMTP-Schnittstelle

Wenn Sie auf Amazon SES über die SMTP-Schnittstelle zugreifen, müssen Sie Ihre Verbindung mit Transport Layer Security (TLS) verschlüsseln. Beachten Sie, dass TLS häufig mit dem Namen des Vorgängerprotokolls, Secure Sockets Layer (SSL), bezeichnet wird.

Amazon SES unterstützt zwei Mechanismen zum Einrichten einer TLS-verschlüsselten Verbindung: STARTTLS und TLS Wrapper.

- STARTTLS – STARTTLS ist ein Verfahren zum Upgraden einer unverschlüsselten Verbindung zu einer verschlüsselten Verbindung. Es stehen Versionen von STARTTLS für eine Reihe von Protokollen zur Verfügung. Die SMTP-Version ist in RFC 3207 definiert. Für STARTTLS-Verbindungen unterstützt Amazon SES TLS 1.2 und TLS 1.3.

- TLS Wrapper – TLS Wrapper (auch bekannt als SMTPS oder Handshake Protocol) ist ein Verfahren zum Initiieren einer verschlüsselten Verbindung, ohne zuvor eine unverschlüsselte Verbindung herzustellen. Bei TLS Wrapper werden vom Amazon-SES-SMTP-Endpunkt keine TLS-Aushandlungen durchgeführt. Es liegt in der Verantwortung des Clients, eine Verbindung mit dem Endpunkt über TLS herzustellen und TLS dann für die gesamte Konversation weiterzuverwenden. TLS Wrapper ist ein älteres Protokoll, wird jedoch von vielen Clients weiterhin unterstützt. Für TLS Wrapper-Verbindungen unterstützt Amazon SES TLS 1.2 und TLS 1.3.

Weitere Informationen zum Herstellen einer Verbindung mit der SMTP-Schnittstelle von Amazon SES mithilfe dieser Methoden finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt.

Amazon SES an Empfänger

Obwohl TLS 1.3 unsere Standardzustellungsmethode ist, kann SES E-Mails mit früheren Versionen von TLS an Mailserver senden.

Standardmäßig verwendet Amazon SES opportunistische TLS. Opportunistic TLS in SES verwendet immer STARTTLS und beinhaltet nicht den TLS-Wrapper. Der Ablauf beinhaltet den Aufbau einer ersten Klartext-Verbindung, gefolgt von einem Upgrade auf eine TLS-verschlüsselte Sitzung, sofern sowohl der Client als auch der Server STARTTLS unterstützen. Wenn SES keine sichere Verbindung herstellen kann, sendet es die Nachricht unverschlüsselt.

Sie können dieses Verhalten ändern, indem Sie Konfigurationssätze verwenden. Verwenden Sie die PutConfigurationSetDeliveryOptionsAPI-Operation, um die `TlsPolicy` Eigenschaft für eine Konfiguration auf `Require` festzulegen. Sie können zur Vornahme dieser Änderung die AWS CLI verwenden.

So konfigurieren Sie Amazon SES so, dass TLS-Verbindungen für einen Konfigurationssatz erforderlich sind.

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 put-configuration-set-delivery-options --configuration-set-
name MyConfigurationSet --tls-policy REQUIRE
```

  Ersetzen Sie es im vorherigen Beispiel *MyConfigurationSet* durch den Namen Ihres Konfigurationssatzes.

Wenn Sie unter Verwendung dieses Konfigurationssatzes eine E-Mail senden, sendet Amazon SES nur die Nachricht nur dann zum empfangenden E-Mail-Server, wenn eine sichere Verbindung hergestellt werden kann. Wenn Amazon SES keine sichere Verbindung mit dem empfangenden E-Mail-Server herstellen kann, wird die Nachricht verworfen.

End-to-end Verschlüsselung

Sie können Amazon SES verwenden, um Nachrichten zu senden, die mit S/MIME oder PGP verschlüsselt sind. Nachrichten, die diese Protokolle verwenden, werden vom Sender verschlüsselt. Ihre Inhalte können nur von Empfängern angezeigt werden, die die privaten Schlüssel besitzen, die zum Entschlüsseln der Nachrichten erforderlich sind.

Amazon SES unterstützt die folgenden MIME-Typen, mit denen Sie S/MIME verschlüsselte E-Mails versenden können:

- `application/pkcs7-mime`
- `application/pkcs7-signature`
- `application/x-pkcs7-mime`
- `application/x-pkcs7-signature`

Amazon SES unterstützt außerdem die folgenden MIME-Typen, mit denen Sie PGP-verschlüsselte E-Mails senden können:

- `application/pgp-encrypted`
- `application/pgp-keys`
- `application/pgp-signature`

Amazon SES Header-Felder

Amazon SES kann alle E-Mail-Header akzeptieren, die das in RFC 822 beschriebene Format aufweisen.

Die folgenden Felder können nicht mehr als einmal im Header-Abschnitt einer Nachricht angezeigt werden:

- `Accept-Language`

- acceptLanguage
- Archived-At
- Auto-Submitted
- Bounces-to
- Comments
- Content-Alternative
- Content-Base
- Content-Class
- Content-Description
- Content-Disposition
- Content-Duration
- Content-ID
- Content-Language
- Content-Length
- Content-Location
- Content-MD5
- Content-Transfer-Encoding
- Content-Type
- Date
- Delivered-To
- Disposition-Notification-Options
- Disposition-Notification-To
- DKIM-Signature
- DomainKey-Signature
- Errors-To
- From
- Importance
- In-Reply-To
- Keywords

- List-Archive
- List-Help
- List-Id
- List-Owner
- List-Post
- List-Subscribe
- List-Unsubscribe
- List-Unsubscribe-Post
- Message-Context
- Message-ID
- MIME-Version
- Organization
- Original-From
- Original-Message-ID
- Original-Recipient
- Original-Subject
- Precedence
- Priority
- References
- Reply-To
- Return-Path
- Return-Receipt-To
- Sender
- Solicitation
- Sensitivity
- Subject
- Thread-Index
- Thread-Topic
- User-Agent

- `VBR-Info`

Überlegungen

- Dieses Feld `acceptLanguage` ist nicht standardmäßig. Sie sollten, wenn möglich, stattdessen den `Accept-Language`-Header verwenden.
- Wenn Sie einen `Date`-Header angeben, überschreibt Amazon SES ihn mit einem Zeitstempel, der dem Datum und der Uhrzeit in der UTC-Zeitzone entspricht, wenn Amazon SES die Nachricht akzeptiert hat.
- Wenn Sie einen `Message-ID`-Header angeben, überschreibt Amazon SES den Header mit dem eigenen Wert.
- Wenn Sie einen `Return-Path`-Header angeben, sendet Amazon SES Unzustellbarkeits- und Beschwerdebenachrichtigungen an die angegebene Adresse. Die Nachricht, die Ihre Empfänger erhalten, enthält jedoch einen anderen Wert für den `Return-Path`-Header.
- Wenn Sie den Amazon SES API `SendEmail` v2-Vorgang mit Simple - oder Templated-Inhalten verwenden oder den `SendBulkEmail` Vorgang verwenden, können Sie keinen benutzerdefinierten Header-Inhalt für Header festlegen, die von SES festgelegt wurden. Daher sind die folgenden Header als benutzerdefinierte Header nicht zulässig:
  - `BCC`, `CC`, `Content-Disposition`, `Content-Type`, `Date`, `From`, `Message-ID`, `MIME-Version`, `Reply-To`, `Return-Path`, `Subject`, `To`

Arbeiten mit E-Mail-Anhängen in SES

E-Mail-Anhänge in SES sind Dateien, die Sie Ihren E-Mail-Nachrichten hinzufügen können, wenn Sie die SES-API v2 `SendEmail` und `SendBulkEmail` -Operationen verwenden. Mit dieser Funktion können Sie Ihre E-Mail-Inhalte um Dokumente wie Word-Dateien PDFs, Bilder oder andere Dateitypen erweitern, die den von SES unterstützten MIME-Typen entsprechen. Sie können auch Inline-Bilder hinzufügen, die direkt in den E-Mail-Inhalt gerendert werden, ohne dass die Empfänger sie separat herunterladen müssen. Sie können mehrere Anlagen pro E-Mail hinzufügen, bis zu einer Gesamtgröße von 40 MB.

> **Note**
>
> `SendEmail`SES API v2 mit `Raw` Inhaltstyp, SMTP-Schnittstelle und SES API v1 verarbeiten Anlagen weiterhin mithilfe der Erstellung von MIME-Rohnachrichten für E-Mails.

So funktionieren Anlagen in SES

Es gibt zwei verschiedene Arten der Verschlüsselung, die in unterschiedlichen Phasen beim Senden einer E-Mail mit Anhängen auftreten:

Phase 1 — Senden von Daten an SES:

- Wenn Sie einen Anhang an SES senden möchten, müssen die Binärdaten (wie ein PDF oder ein Bild) in ein Format konvertiert werden, das sicher übertragen werden kann.
- Hier kommt die Base64-Kodierung ins Spiel — sie ist erforderlich, da Sie in einer JSON-Anfrage keine binären Rohdaten senden können.
- Wenn Sie das AWS SDK verwenden, verarbeitet es diese Kodierung automatisch.
- Wenn Sie das verwenden AWS CLI, müssen Sie den Anhang vor dem Senden selbst base64-kodieren.

Phase 2 — SES erstellt die E-Mail:

- Sobald SES Ihre Daten erhalten hat, muss es eine tatsächliche E-Mail mit dem Anhang erstellen.
- Hier kommt die ContentTransferEncodingEinstellung ins Spiel.
- SES verwendet die von Ihnen angegebene Verschlüsselungsmethode ContentTransferEncoding , um den Anhang in der endgültigen E-Mail automatisch zu formatieren.

Stellen Sie sich das so vor — es ist vergleichbar mit dem Versenden eines Pakets per Post. Zuerst müssen Sie das Paket zur Post bringen (Stufe 1 — Base64-Kodierung erforderlich), dann verpackt das Postamt es entsprechend für die endgültige Zustellung (Stufe 2 —). ContentTransferEncoding

Struktur des Anhangsobjekts

Wenn Sie eine E-Mail mit Anhängen über SES senden, verarbeitet der Dienst die komplexe Konstruktion von MIME-Nachrichten automatisch. Sie müssen lediglich den Inhalt und die Metadaten des Anhangs über die folgende `Attachment`SES-API-v2-Objektstruktur bereitstellen:

- `FileName`(Erforderlich) — Der den Empfängern angezeigte Dateiname (muss die Dateierweiterung enthalten). Falls nicht angegeben, leitet SES a `ContentType` aus der Erweiterung von ab. `FileName`
- `ContentType`(Optional) — IANA-konforme Medientyp-ID.

- `ContentDisposition`(Optional) — Gibt an, wie der Anhang gerendert werden soll: `ATTACHMENT` (Standard) oder. `INLINE`
- `ContentDescription`(Optional) — Kurze Beschreibung des Inhalts.
- `RawContent`(Erforderlich) — Der tatsächliche Inhalt des Anhangs.
- `ContentTransferEncoding`(Optional) — Gibt an, wie die Nutzdaten des Anhangs kodiert werden, wenn sie zur MIME-Nachricht der E-Mail zusammengefügt werden: `SEVEN_BIT` (Standard), *`BASE64`* oder. `QUOTED_PRINTABLE`

Der gesamte angehängte Inhalt muss Base64-kodiert werden, bevor er zum Senden an den SES-Endpunkt übertragen wird. Wenn Sie den AWS SDK-Client für API-Aufrufe verwenden, wird dies automatisch für Sie erledigt. Wenn Sie den AWS CLI Client verwenden oder Ihren eigenen implementiert haben, müssen Sie die Kodierung selbst vornehmen, z. B.:

- Klartextinhalt: `Text attachment sample content.`
- Base64-kodiert: `VGV4dCBhdHRhY2htZW50IHNhbXBsZSBjb250ZW50Lg==`

Die folgenden Beispiele zeigen, wie die Anlagenobjektstruktur bei der Spezifizierung von Anhängen mit der SES-API v2 `SendEmail`und bei `SendBulkEmail`Vorgängen verwendet wird, bei denen auf eine JSON-Datei AWS CLI verwiesen wird, die Elemente von Anhangsobjekten enthält.

Example— SendEmail mit einfachem Inhalt

```
aws sesv2 send-email --cli-input-json file://request-send-email-simple.json
```

request-send-email-simple.json

```
{
    "FromEmailAddress": "sender@example.com",
    "Destination": {
        "ToAddresses": [
            "recipient@example.com"
        ]
    },
    "Content": {
        "Simple": {
            "Subject": {
                "Data": "Email with attachment"
```

```
            },
            "Body": {
                "Text": {
                    "Data": "Please see attached document."
                },
                "Html": {
                    "Data": "Please see attached <b>document</b>."
                }
            },
            "Attachments": [
                {
                    "RawContent": "<base64-encoded-content>",
                    "ContentDisposition": "ATTACHMENT",
                    "FileName": "document.pdf",
                    "ContentDescription": "PDF Document Attachment",
                    "ContentTransferEncoding": "BASE64"
                }
            ]
        }
    }
}
```

Example— SendEmail mit einfachem Inhalt und Inline-Anhang

```
aws sesv2 send-email --cli-input-json file://request-send-email-simple-inline-
attachment.json
```

request-send-email-simple-inline-attachment.json

```
{
    "FromEmailAddress": "sender@example.com",
    "Destination": {
        "ToAddresses": [
            "recipient@example.com"
        ]
    },
    "Content": {
        "Simple": {
            "Subject": {
                "Data": "Email with attachment"
            },
            "Body": {
                "Html": {
```

```
                    "Data": "<html><body>Our logo:<br><img src=\"cid:logo123\" alt=
\"Company Logo\"></body></html>"
                }
            },
            "Attachments": [
                {
                    "RawContent": "<base64-encoded-content>",
                    "ContentDisposition": "INLINE",
                    "FileName": "logo.png",
                    "ContentId": "logo123",
                    "ContentTransferEncoding": "BASE64"
                }
            ]
        }
    }
}
```

Example— mit Vorlageninhalten SendEmail

```
aws sesv2 send-email --cli-input-json file://request-send-email-template.json
```

request-send-email-template.json

```
{
    "FromEmailAddress": "sender@example.com",
    "Destination": {
        "ToAddresses": [
            "recipient@example.com"
        ]
    },
    "Content": {
        "Template": {
            "TemplateName": "MyTemplate",
            "TemplateData": "{\"name\":\"John\"}",
            "Attachments": [
                {
                    "RawContent": "<base64-encoded-content>",
                    "ContentDisposition": "ATTACHMENT",
                    "FileName": "document.pdf",
                    "ContentDescription": "PDF Document Attachment",
                    "ContentTransferEncoding": "BASE64"
                }
            ]
```

```
        }
    }
}
```

Example— SendBulkEmail mit dem Inhalt von Anhängen

```
aws sesv2 send-bulk-email --cli-input-json file://request-send-bulk-email.json
```

request-send-bulk-email.json

```
{
    "FromEmailAddress": "sender@example.com",
    "DefaultContent": {
        "Template": {
            "TemplateName": "MyTemplate",
            "TemplateData": "{}",
            "Attachments": [
                {
                    "RawContent": "<base64-encoded-content>",
                    "ContentDisposition": "ATTACHMENT",
                    "FileName": "document.pdf",
                    "ContentDescription": "PDF Document Attachment",
                    "ContentTransferEncoding": "BASE64"
                }
            ]
        }
    },
    "BulkEmailEntries": [
        {
            "Destination": {
                "ToAddresses": [
                    "recipient@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{\"name\":\"John\"}"
                }
            }
        }
    ]
}
```

Best Practices

- Halten Sie die Gesamtgröße der Nachricht (einschließlich Anlagen) unter 40 MB.
- Lassen Sie SES Inhaltstypen nach Möglichkeit automatisch anhand von Dateierweiterungen erkennen.
- Geben Sie Inhaltstypen nur dann explizit an, wenn sie nicht zu den gängigen MIME-Typen gehören.
- Erwägen Sie die Verwendung von Inline-Bildern für ein besseres E-Mail-Rendering.
- SES unterstützt eine Vielzahl von MIME-Typen für Anlagen, mit Ausnahme der unter aufgeführtenNicht-unterstützte Anhangtypen.

SES unterstützt nicht die Typen von Anhängen

Sie können Nachrichten mit Anhängen über Amazon SES versenden, indem Sie den Multipurpose Internet Mail Extensions (MIME)-Standard verwenden. Amazon SES akzeptiert alle Dateianhangstypen mit Ausnahme von Anhängen mit den Dateierweiterungen in der folgenden Liste.

.ade	.hta	.mau	.mst	.psc1
.adp	.inf	.mav	.ops	.psc2
.app	.ins	.maw	.pcd	.tmp
.asp	.isp	.mda	.pif	.URL
.bas	.its	.mdb	.plg	.vb
.bat	.js	.mde	.prf	.vbe
.cer	.jse	.mdt	.prg	.vbs
.chm	.ksh	.mdw	.reg	.vps
.cmd	.lib	.mdz	.scf	.vsmacros
.com	.lnk	.msc	.scr	.vss
.cpl	.mad	.msh	.sct	.vst

.crt	.maf	.msh1	.shb	.vsw
.csh	.mag	.msh2	.shs	.vxd
.der	.mam	.mshxml	.sys	.ws
.exe	.maq	.msh1xml	.ps1	.wsc
.fxp	.mar	.msh2xml	.ps1xml	.wsf
.gadget	.mas	.msi	.ps2	.wsh
.hlp	.mat	.msp	.ps2xml	.xnk

Für ISPs einige gelten weitere Einschränkungen (z. B. Einschränkungen in Bezug auf archivierte Anlagen). Wir empfehlen Ihnen daher, Ihren E-Mail-Versand über den Hauptmodus zu testen, ISPs bevor Sie Ihre Produktions-E-Mail versenden.

Empfang von E-Mails mit Amazon SES

Sie können Amazon SES nicht nur zur Verwaltung Ihres E-Mail-Versands verwenden, sondern den Service auch so konfigurieren, dass E-Mails im Namen einer oder mehrerer Ihrer Domänen empfangen werden. Wenn Sie SES verwenden, um E-Mails zu empfangen, kümmert sich SES um die zugrundeliegenden Empfangsaktivitäten wie die Kommunikation mit anderen Mailservern, das Scannen nach Spam und Viren, das Blockieren von E-Mails aus nicht vertrauenswürdigen Quellen (die Adressen auf der Blockierungsliste lauten entweder Spamhaus oder SES) und das Annehmen von E-Mails für Empfänger in Ihrer Domäne.

Der Umfang der Verarbeitung Ihrer empfangenen E-Mail wird durch die von Ihnen angegebenen benutzerdefinierten Anweisungen bestimmt. Diese Anweisungen werden in zwei Formen angeboten:

- Receipt rules (Empfangsregeln) (recipient-based control) (Empfängerbasierte Steuerung) bieten die feinste Granularität der Kontrolle über eingehende E-Mails. Mit Empfangsregeln können erweiterte Verarbeitungsvorgänge durchgeführt werden, z. B. eingehende E-Mails an einen Amazon S3-Bucket zugestellt, in einem Amazon SNS SNS-Thema veröffentlicht, an Amazon gesendet oder automatisch Bounce-Nachrichten gesendet werden WorkMail, wenn Nachrichten an bestimmte E-Mail-Adressen gesendet werden, und vieles mehr.
- IP address filters (Filter für die IP-Adressen) (IP-based control) (IP-basierte Steuerung) bieten ein breites Maß an Kontrolle und sind einfach einzurichten. Mit diesen Filtern können Sie alle Nachrichten aus bestimmten IP-Adressen oder IP-Adressbereichen explizit blockieren oder zulassen.

Um mit dem Empfangen von E-Mails, der Einrichtung und der Implementierung zu beginnen, indem Sie entweder -Empfangsregeln oder Filter für die IP-Adressen, zuerst durchlesenE-Mail-Empfangskonzepte & Anwendungsfälle, um einen Überblick darüber zu erhalten, wie es funktioniert und wie Sie es verwenden können. Danach führt Einrichten des E-Mail-Empfangs in Sie durch die Voraussetzungen für die Einrichtung des E-Mail-Empfangs. Dann führt Exemplarische Vorgehensweisen für die E-Mail-Empfangskonsole Sie durch die Assistenten, die für die Konfiguration von -Empfangsregeln und Filter für die IP-Adressen verwendet werden.

> **Note**
>
> Der E-Mail-Empfang kann nur verwendet werden, wenn sich Ihr Konto in einem Land befindet, in AWS-Region dem SES den E-Mail-Empfang unterstützt. In der Tabelle mit den

E-Mail-Empfangsendpunkten in der Tabelle Allgemeine AWS-Referenz sind alle Endpunkte aufgeführt, in AWS-Regionen denen SES den E-Mail-Empfang unterstützt.

Themen in diesem Abschnitt:

- Amazon SES-Konzepte für den E-Mail-Empfang
- Einrichten des Amazon-SES-E-Mail-Empfangs
- Amazon SES E-Mail-Empfangskonsole — exemplarische Vorgehensweisen
- Anzeigen von Metriken für den Amazon-SES-E-Mail-Empfang

Amazon SES-Konzepte für den E-Mail-Empfang

Wenn Sie Amazon SES als E-Mail-Receiver verwenden, müssen Sie dem Service Anweisungen geben, wie mit Ihren E-Mails zu verfahren ist. Die primäre Methode, Empfangsregeln, ermöglicht eine abgestimmte Kontrolle über Ihren E-Mail-Empfang, indem SieEmpfängerbasiertes Steuerelement, um eine Reihe von Aktionen anzugeben, die basierend auf dem Empfänger ausgeführt werden sollen. Die andere Methode, IP-Adressfilter, bietet eine breite Ebene vonIP-basierte Steuerung, um E-Mails basierend auf der ursprünglichen IP-Adresse oder dem IP-basierten Adressbereich zu blockieren oder zuzulassen.

Diese beiden Methoden werden in diesem Abschnitt beschrieben, zusammen mit einer Übersicht darüber, wie Amazon SES empfangene E-Mails verarbeitet, und Anwendungsfälle, die Ihnen helfen, beim Einrichten von Regeln und Filtern Ihre E-Mails zu empfangen, zu filtern und zu verarbeiten.

Themen in diesem Abschnitt:

- Empfängerbasierte Steuerung mit Zahlungsregeln
- IP-basierte Steuerung mit IP-Adressfiltern
- E-Mail-Empfangsprozess
- Anwendungsfälle und Einschränkungen für den Erhalt Amazon SES E-Mails
- E-Mail-Empfang von Authentifizierung und Malware-Scan

Empfängerbasierte Steuerung mit Zahlungsregeln

Die primäre Möglichkeit, Ihre eingehenden E-Mails zu steuern, besteht darin, anzugeben, wie E-Mails über eine geordnete Liste von Aktionen für Ihre verifizierten Identitäten, zu denen Domänen,

Unterdomänen oder E-Mail-Adressen gehören, behandelt werden. Beachten Sie, dass die E-Mail-Adressen zu einer Ihrer verifizierten Domänenidentitäten gehören müssen. Diese Aktionen sind definiert und in Empfangsregeln, die Sie innerhalb eines Regelsatzes erstellen.

Als Option können Sie auch Empfängerbedingungen hinzufügen, um anzugeben, dass die Aktionen nur ausgeführt werden, wenn der Empfänger, an den die eingehende E-Mail adressiert ist, mit einer Empfängeridentität übereinstimmt, die in der Bedingung festgelegt ist. Sind Sie beispielsweise im Besitz der Domäne example.com, können Sie angeben, dass E-Mails für user@example.com unzustellbar sind und alle anderen E-Mails für example.com und ihre Subdomänen zugestellt werden sollen.

Andernfalls, wenn Sie keine Empfängerbedingungen hinzufügen, werden die Aktionen auf alle E-Mail-Adressen, Domänen und Unterdomänen angewendet, die zu Ihren verifizierten Domänen gehören. Die folgenden Aktionen können auf Ihre Zahlungsregeln angewendet werden:

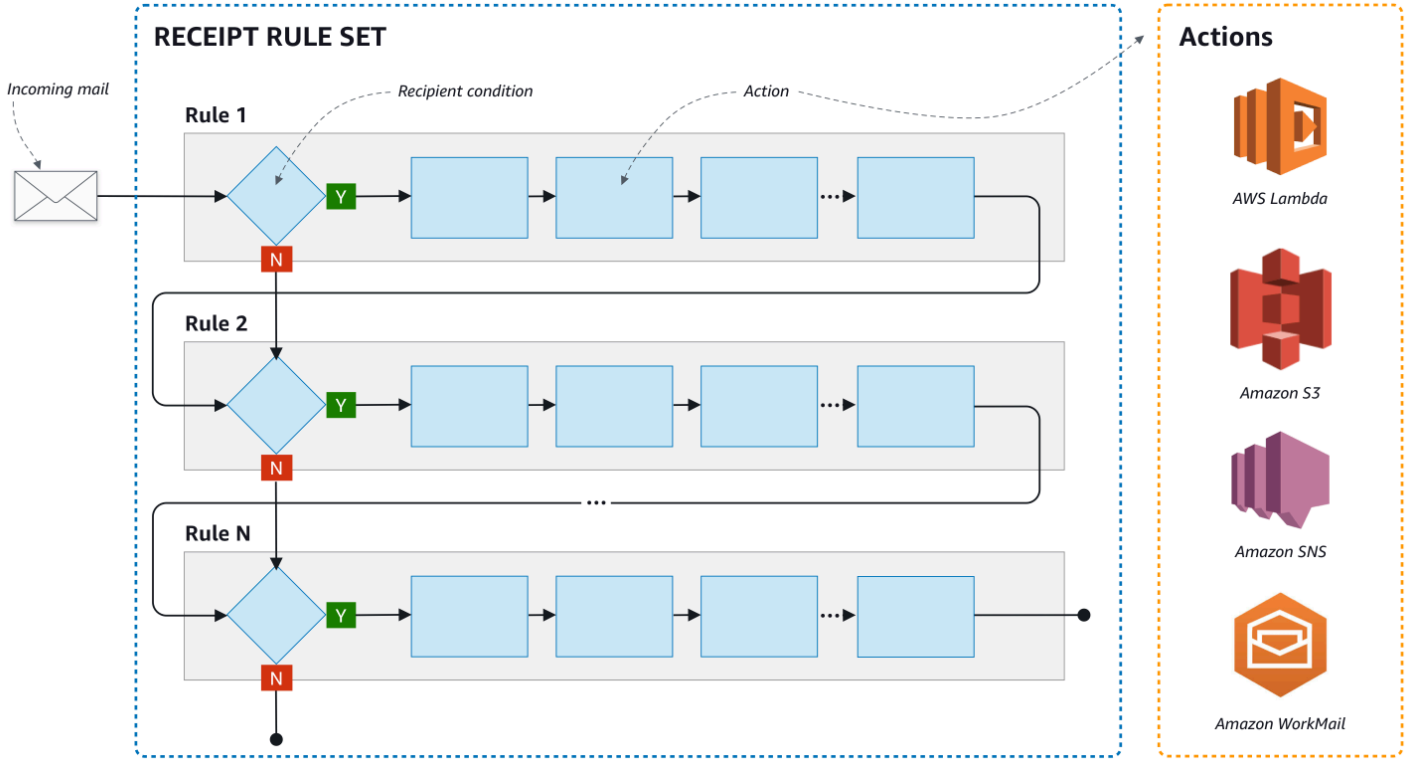
- "Add Header"-Aktion – Fügt der empfangenen E-Mail einen Header hinzu. Diese Aktion wird normalerweise nur in Kombination mit anderen Aktionen verwendet.
- Return bounce response action (Aktion Unzustellbarkeitsantwort ablehnen) – Lehnt die E-Mail mit einer Unzustellbarkeitsnachricht an den Sender ab und benachrichtigt Sie optional über Amazon SNS.
- AWS Lambda Funktionsaktion aufrufen — Ruft Ihren Code über eine Lambda-Funktion auf und benachrichtigt Sie optional über Amazon SNS.
- Deliver to S3 bucket action (Aktion zu S3-Bucket bereitstellen) – Stellt die E-Mail einem Amazon S3-Bucket zu und benachrichtigt Sie optional über Amazon SNS.
- Aktion zum Veröffentlichen in Amazon SNS -Thema —Veröffentlichen der E-Mail in einem Amazon SNS -Thema.

  > **Note**
  >
  > Die SNS-Aktion beinhaltet eine vollständige Kopie der E-Mail-Inhalte in den Amazon SNS-Benachrichtigungen. Die anderen hier genannten Amazon SNS-Benachrichtigungen dienen dazu, Sie über die E-Mail-Zustellung zu informieren. Sie enthalten Informationen über die E-Mail, nicht die eigentlichen E-Mail-Inhalte.

- "Stop"-Aktion – Beendet die Auswertung des Empfangsregelsatzes und benachrichtigt Sie optional über Amazon SNS.

- Mit WorkMail Amazon-Aktion integrieren — Verarbeitet die Post mit Amazon WorkMail. In der Regel werden Sie diese Aktion nicht direkt verwenden, da Amazon sich um die Einrichtung WorkMail kümmert.

Empfangsregeln werden in Empfangsregelsätze gruppiert. Wenn Sie über keinen vorhandenen Regelsatz verfügen, müssen Sie zunächst einen Regelsatz erstellen, bevor Sie mit dem Erstellen von Zahlungsregeln beginnen. Sie können mehrere Regelsätze für Ihr AWS Konto definieren, es ist jedoch immer nur ein Regelsatz aktiv. Die folgende Abbildung zeigt, wie Empfangsregeln, Empfangsregelsätze und Aktionen miteinander in Beziehung stehen.



IP-basierte Steuerung mit IP-Adressfiltern

Sie können Ihren E-Mail-Verkehr auf einer breiteren Ebene durch Einrichten von IP-Adressenfilter kontrollieren. IP-Adressenfilter sind optional und ermöglichen Ihnen, anzugeben, ob E-Mails, die von einer IP-Adresse oder aus einem IP-Adressbereich stammen, akzeptiert oder blockiert werden sollen. Ihre IP-Adressenfilter können Blockierungslisten (IP-Adressen, von denen Sie eingehende E-Mails blockieren möchten) und Freigabelisten (IP-Adressen, von denen Sie die E-Mails immer akzeptieren möchten) umfassen.

IP-Adressenfilter sind nützlich, um Spam zu blockieren. Amazon SES unterhält eine eigene Blockierungsliste mit IP-Adressen, die für das Senden von Spam bekannt sind. Sie können jedoch festlegen, ob E-Mails von diesen IP-Adressen empfangen werden sollen, indem Sie sie in Ihre Zulassungsliste aufnehmen. Da es keine Protokolle gibt, die zeigen, welche IP-Adressen blockiert werden, muss der gesperrte Absender Sie informieren. Dies ist auch eine gute Gelegenheit, dem Absender zu helfen, festzustellen, ob sich seine IP-Adresse in einer Blockierungsliste wie Spamhaus befindet, und ihm zu empfehlen, einen Antrag zu stellen, von der Liste entfernt zu werden. Dies ist sowohl für Sie als auch für den Absender von Vorteil, da Sie keinen IP-Adressfilter für ihn pflegen müssen und der Absender seine E-Mail-Zustellbarkeit verbessern kann.

> **Note**
>
> - Unabhängig von Ihrer IP-Adressfilterkonfiguration blockiert Amazon EC2 ausgehenden Datenverkehr auf Port 25 (E-Mail-Versand), sofern dieser nicht auf die Zulassungsliste gesetzt wurde. Weitere Informationen finden Sie in diesem AWS re:Post-Artikel.
> - Wenn Sie nur E-Mails von einer endlichen Liste bekannter IP-Adressen erhalten möchten, richten Sie eine Blockierungsliste mit `0.0.0.0/0` und eine Freigabeliste ein, die die IP-Adressen enthält, denen Sie vertrauten. Diese Konfiguration blockiert alle IP-Adressen standardmäßig und lässt nur E-Mails von den IP-Adressen zu, die Sie explizit angeben.

E-Mail-Empfangsprozess

Wenn Amazon SES eine E-Mail für Ihre Domäne empfängt, treten die folgenden Ereignisse ein:

1. Amazon SES sucht zuerst die IP-Adresse des Senders. Amazon SES erlaubt, dass die E-Mail diese Stufe passiert, es sei denn:
   - Die IP-Adresse ist in Ihrer Blockierungsliste enthalten.
   - Die IP-Adresse ist in der Amazon SES-Blockierungsliste und nicht in Ihrer Freigabeliste aufgeführt.
2. Amazon SES untersucht Ihren aktiven Empfangsregelsatz, um zu ermitteln, ob Ihre Empfangsregeln eine Bedingung enthalten, die einem der Empfänger der eingehenden E-Mail entspricht.
   - Wenn es eine Empfängerbedingung gibt und sie mit einem der Empfänger der eingehenden E-Mail übereinstimmt, akzeptiert Amazon SES die E-Mail. Wenn es keine Übereinstimmungen gibt, blockiert Amazon SES die E-Mail.

- Wenn die Zahlungsregel keine Empfängerbedingung enthält, akzeptiert Amazon SES die E-Mail. Alle Aktionen der Regel gelten für alle verifizierten Identitäten, die Sie besitzen.

3. Amazon SES authentifiziert die E-Mail und scannt ihren Inhalt auf Spam und Malware:
   - Die IP-Adresse des Remote-Hosts, der die E-Mail an Amazon SES gesendet hat, wird mit der SPF-Richtlinie verglichen, die unter der Domäne von MAIL FROM angegeben wurde, die während der SMTP-Transaktion verwendet wurde.
   - Die DKIM-Signaturen im Header-Bereich der E-Mail werden überprüft.
   - Wenn das Scannen von Inhalten aktiviert ist, wird der E-Mail-Inhalt auf Spam und Malware gescannt.
   - Die Ergebnisse der E-Mail-Authentifizierung und der Inhaltsüberwachung werden Ihnen während der Auswertung der Empfangsregeln zur Verfügung gestellt.

   Weitere Informationen finden Sie unter E-Mail-Authentifizierung und Malware-Erkennung.
4. Für die E-Mail, die Amazon SES akzeptiert, werden alle Zahlungsregeln innerhalb Ihres aktiven Regelsatzes in der von Ihnen definierten Reihenfolge angewendet. Innerhalb jeder Zahlungsregel werden die Aktionen in der von Ihnen definierten Reihenfolge ausgeführt.

Anwendungsfälle und Einschränkungen für den Erhalt Amazon SES E-Mails

In diesem Abschnitt werden einige allgemeine Überlegungen und Anwendungsfälle für den Empfang von Amazon SES E-Mails behandelt. Im Frage- und Antwortformat werden häufig gestellte Fragen und Fakten vorgestellt, um festzustellen, ob es von Vorteil wäre, dass Amazon SES E-Mails im Namen einer oder mehrerer verifizierter Domänen empfangen und verwalten kann, die Sie besitzen.

Regionale Verfügbarkeit

Unterstützt Amazon SES das Empfangen von E-Mails in Ihrer Region?

Amazon SES unterstützt den E-Mail-Empfang nur in bestimmten AWS Regionen. Eine vollständige Liste der Regionen, in denen der E-Mail-Empfang unterstützt wird, finden Sie unter Endpunkte und Kontingente von Amazon Simple Email Service in der Allgemeine AWS-Referenz.

POP- oder IMAP-basierte E-Mail-Clients

Kann Microsoft Outlook zum Empfangen eingehender E-Mails verwendet werden?

Amazon SES enthält keine POP- oder IMAP-Server für den Empfang eingehender E-Mails. Dies bedeutet, dass Sie keinen E-Mail-Client wie beispielsweise Microsoft Outlook zum Empfangen

eingehender E-Mails verwenden können. Wenn Sie eine Lösung benötigen, mit der Sie mithilfe eines E-Mail-Clients sowohl E-Mails senden als auch empfangen können, sollten Sie Amazon in Betracht ziehen WorkMail.

Nutzung anderer AWS Dienste

Haben Sie die entsprechenden Berechtigungen einrichten?

Wenn Sie möchten, dass Ihre E-Mail-Nachrichten einem Amazon-S3-Bucket zugestellt werden, in einem nicht eigenen Amazon-SNS-Thema veröffentlicht werden, eine Lambda-Funktion auslösen oder einen benutzerdefinierten -Hauptschlüssel verwenden, müssen Sie Amazon SES die Berechtigung für den Zugriff auf diese Ressourcen erteilen. Um Amazon SES Zugriff zu gewähren, erstellen Sie Richtlinien für Ressourcen auf den Konsolen oder APIs für diese AWS Services. Weitere Informationen finden Sie unter Erteilen von Berechtigungen.

E-Mail-Inhalt

Wie soll Amazon SES Ihnen die E-Mail-Inhalte übergeben?

Amazon SES kann Ihnen die E-Mail-Inhalte auf zwei Arten bereitstellen: Entweder werden die E-Mails in einem von Ihnen angegebenem Amazon-S3-Bucket gespeichert oder Sie erhalten eine Amazon-SNS-Benachrichtigung mit einer Kopie der E-Mail. Amazon SES stellt Ihnen die unformatierte, ungeänderte E-Mail zu, die in der Regel das Format Multipurpose Internet Mail Extensions (MIME) hat. Weitere Informationen zum MIME-Format finden Sie unter RFC 2045.

Wie groß sind die E-Mails, die Sie erhalten werden?

Wenn Sie Ihre E-Mails in einem S3-Bucket speichern, beträgt die maximale E-Mail-Größe (einschließlich Header) 40 MB. Wenn Sie Ihre E-Mails über Amazon-SNS-Benachrichtigungen erhalten, beträgt die maximale E-Mail-Größe (einschließlich Header) 150 KB.

Wie soll die Verarbeitung Ihrer E-Mail ausgelöst werden?

Nachdem Ihre E-Mail zugestellt wurde, möchten Sie sie mit Ihrem eigenen Code verarbeiten. Ihre Anwendung kann beispielsweise die Base64-kodierten E-Mails in ein anzeigbares Format konvertieren und sie einem Endbenutzer dann über einen E-Mail-Client verfügbar machen. Es gibt mehrere Möglichkeiten, diesen Prozess zu starten:

- Wenn Ihre E-Mails an Amazon S3 übermittelt werden, kann Ihre Anwendung von S3-Aktionen generierte Amazon-SNS-Benachrichtigungen empfangen, die Mitteilungs-ID der E-Mail aus den Benachrichtigungen extrahieren und die E-Mail mithilfe der Mitteilungs-ID aus Amazon S3 abrufen.

Alternativ können Sie die E-Mail-Verarbeitung in Ihre Empfangsregeln integrieren, indem Sie eine Lambda-Funktion schreiben. In diesem Fall sollte Ihre Empfangsregel die E-Mail zuerst in Amazon S3 schreiben und dann die Lambda-Funktion auslösen. Lambda-Aktionen können über Ihre Empfangsregeln synchron oder asynchron ausgeführt werden, je nachdem, ob die Lambda-Funktion ein Ergebnis zurückgeben muss, das die Ausführung anderer Aktionen beeinflusst. Wir empfehlen, dass Sie die asynchrone Ausführung verwenden, es sei denn, für Ihren Anwendungsfall ist synchron unbedingt notwendig. Weitere Informationen AWS Lambda dazu finden Sie im AWS Lambda Entwicklerhandbuch.

- Wenn Ihre E-Mails über eine Amazon-SNS-Benachrichtigung mit der SNS-Aktion zugestellt werden, kann Ihre Anwendung Amazon-SNS-Benachrichtigungen empfangen und dann die E-Mail-Nachrichten aus den Benachrichtigungen extrahieren.

Möchten Sie, dass die E-Mails verschlüsselt werden?

Amazon SES lässt sich in AWS Key Management Service (AWS KMS) integrieren, um optional die E-Mails zu verschlüsseln, die es in Ihren S3-Bucket schreibt. Amazon SES nutzt die clientseitige Verschlüsselung, um Ihre E-Mail zu verschlüsseln, bevor sie in Amazon S3 geschrieben wird. Dies bedeutet, dass Sie den Inhalt Ihrerseits entschlüsseln müssen, nachdem Sie die E-Mail von Amazon S3 abgerufen haben. AWS SDK für Java und AWS SDK für Ruby stellen einen Client bereit, der die Entschlüsselung für Sie übernehmen kann. Amazon SES kann die E-Mails nur für Sie entschlüsseln, wenn Sie auswählen, Ihre E-Mail-Nachrichten an einen Amazon-S3-Bucket zustellen zu lassen.

Unerwünschte E-Mail

An welchem Punkt des E-Mail-Empfangsprozesses möchten Sie unerwünschte E-Mails blockieren?

Wenn ein Absender versucht, eine E-Mail an einen Empfänger zu senden, tauscht der E-Mail-Server des Absenders mit dem Server des Empfängers eine Sequenz von Befehlen aus. Diese Sequenz wird als SMTP-Aushandlung bezeichnet.

Sie können eingehende E-Mails an zwei Punkten des E-Mail-Empfangsprozesses blockieren – während der SMTP-Aushandlung und nach der SMTP-Aushandlung. Verwenden Sie IP-Adressenfilter, um Nachrichten während der SMTP-Aushandlung zu blockieren, und Empfangsregeln zum Blockieren von E-Mails nach der SMTP-Aushandlung.

Mit IP-Adressenfiltern können Sie E-Mails blockieren, die von bestimmten IP-Adressen stammen. Das Blockieren unerwünschter E-Mails mit Hilfe von IP-Adressenfiltern hat den Vorteil, dass für Nachrichten, die während der SMTP-Aushandlung blockiert werden, keine Gebühren anfallen. Der

Nachteil der Verwendung von IP-Adressenfiltern besteht darin, dass die E-Mails der angegebenen IP-Adressen ohne Analyse des tatsächlichen Inhalts blockiert werden. Weitere Informationen zu IP-Adressfiltern finden Sie unter Exemplarische Vorgehensweise bei der Konfiguration von IP-Adressenfiltern.

Sie können Empfangsregeln nutzen, um basierend auf der Adresse (oder Domäne bzw. Subdomäne), an die die Nachricht gesendet wurde, eine Unzustellbarkeitsbenachrichtigung an den Absender zu senden. Der Vorteil der Verwendung von Empfangsregeln besteht darin, dass Sie weitere Analysen eingehender Nachrichten durchführen können, bevor Sie eine Unzustellbarkeitsbenachrichtigung an den Absender schicken. Sie können es beispielsweise verwenden, AWS Lambda um Bounce-Benachrichtigungen nur dann zu versenden, wenn Nachrichten die DKIM-Authentifizierung nicht bestehen oder als Spam identifiziert werden. Der Nachteil der Verwendung von Empfangsregeln besteht darin, dass Empfangsregeln erst nach der SMTP-Aushandlung verarbeitet werden, weshalb Ihnen jede empfangene Nachricht in Rechnung gestellt wird. Es können auch Kosten anfallen, wenn Sie Lambda verwenden, um den Inhalt der eingehenden Nachrichten zu analysieren. Weitere Informationen zu Empfangsregeln finden Sie unter Exemplarische Vorgehensweise in der Konsole für Zahlungsregeln erstellen. Weitere Informationen zur Verwendung von Lambda für die Analyse eingehender E-Mails finden Sie unter Beispiele für Lambda-Funktionen.

E-Mail-Streams

Wie möchten Sie den E-Mail-Stream teilen?

Ihre Domäne empfängt wahrscheinlich E-Mail verschiedener Klassen. Ein Teil der E-Mail Ihrer Domäne, z. B. eine E-Mail an den user@example.com, kann beispielsweise an ein privates Postfach gerichtet sein. Andere E-Mails, z. B. eine E-Mail an unsubscribe@example.com, ist stattdessen eher für automatisierte Systeme bestimmt. Sie können Ihre eingehenden E-Mails mithilfe von Empfangsregeln teilen, sodass sie unterschiedlich verarbeitet werden können. Weitere Informationen zum Einrichten von Empfangsregeln finden Sie unter Erstellen von Empfangsregeln.

E-Mail-Empfang von Authentifizierung und Malware-Scan

Amazon SES authentifiziert jede empfangene E-Mail und scannt optional den Inhalt der E-Mail auf Spam und Malware. SES ergreift keine Maßnahmen für empfangene E-Mails basierend auf den Ergebnissen der E-Mail-Authentifizierung oder des Inhaltsscans. Die Ergebnisse dieser Vorgänge werden Ihnen jedoch als Attribute zur Verfügung gestellt, die Sie in SES-Empfangsregelaktionen wie Amazon-SNS-Benachrichtigungen oder als Header in einer Nachricht übermittelt an Amazon S3 verwenden können.

E-Mail-Authentifizierung

Amazon SES authentifiziert jede empfangene E-Mail mit SPF, DKIM und DMARC. Die Ergebnisse jedes Authentifizierungsmechanismus finden Sie in den Amazon-SNS-Benachrichtigungen, die SES im Rahmen der Auswertung der Regeln im aktiven Empfangsregelsatz versendet. Wenn Sie sich außerdem dafür entschieden haben, eine Kopie der E-Mail in Amazon S3 zu erhalten, wird das Ergebnis der E-Mail-Authentifizierung im `Authentication-Results`-Header erfasst, den SES dem Header-Abschnitt der E-Mail hinzufügt:

```
Authentication-Results: example.com;
spf=pass (spfCheck: 10.0.0.1 is permitted by domain of example.com) client-ip=10.0.0.1;
 envelope-from=example@example.com; helo=10.0.0.1;
dkim=pass header.i=example.com;
dkim=permerror header.i=some-example.com;
dmarc=pass header.from=example@example.com;
```

Der `Authentication-Results`-Header ist in RFC 8601 beschrieben

Scannen von E-Mail-Inhalten auf Spam- und Malware-Erkennung

Amazon SES scannt empfangene E-Mail-Inhalte auf Malware, abhängig vom Wert des Attributs ScanEnabled(API) oder des Spam- und Virenscans (Konsole) der Empfangsregel, die der E-Mail entsprach. Standardmäßig scannt SES empfangene E-Mail-Inhalte auf Malware. Um die Inhaltsüberprüfung für empfangene E-Mails zu deaktivieren, die einer bestimmten Empfangsregel entsprechen, müssten Sie bei Verwendung der API die ScanEnabledMarkierung der Empfangsregel auf Falsch setzen oder bei Verwendung der Konsole das Kontrollkästchen Spam- und Virenscans deaktivieren. Wenn die Empfangsregel, die mit einer E-Mail übereinstimmte, Scan aktiviert ist, wird das Ergebnis des Inhaltsscans in den Amazon-SNS-Benachrichtigungen bereitgestellt, die SES im Rahmen der Bewertung der Regeln im aktiven Empfangsregelsatz versendet. Wenn Sie sich außerdem dafür entschieden haben, eine Kopie der E-Mail in Amazon S3 zu erhalten, wird das Ergebnis des Inhaltsscans in den `X-SES-Spam-Verdict-` und `X-SES-Virus-Verdict`-Headern erfasst, die SES dem Header-Abschnitt der E-Mail hinzufügt.

```
X-SES-Spam-Verdict: PASS
X-SES-Virus-Verdict: FAIL
```

Die möglichen Werte für die obigen Header sind aufgeführt in:

- Spam
- Virus

Nachdem Sie sich die Konzepte für den Empfang von E-Mails verstanden haben, wie es funktioniert und die Anwendungsfälle sind, können Sie die ersten Schritte unter Einrichten des E-Mail-Empfangs in starten.

Einrichten des Amazon-SES-E-Mail-Empfangs

In diesem Abschnitt werden die Voraussetzungen beschrieben, die erforderlich sind, bevor Sie mit der Konfiguration von Amazon SES für den Empfang Ihrer E-Mails beginnen können. Es ist wichtig, dass SieE-Mail-Empfangskonzepte & AnwendungsfälleUm die Konzepte zur Funktionsweise von Amazon SES zu verstehen und darüber nachzudenken, wie Sie Ihre E-Mails erhalten, filtern und verarbeiten möchten.

Bevor Sie den E-Mail-Empfang konfigurieren können, indem Sie eineRegelsatz,Empfangsregeln, undIP-AdressenfilterSie müssen zuerst die folgenden Einrichtungsvoraussetzungen erfüllen:

- Verifizieren Sie mit Amazon SES Ihre Domäne, indem Sie DNS-Einträge veröffentlichen, um nachzuweisen, dass diese Ihnen gehört.
- Erlauben Sie Amazon SES, E-Mails für Ihre Domain zu erhalten, indem Sie einen MX-Eintrag veröffentlichen.
- Erteilen Sie Amazon SES die Erlaubnis, auf andere AWS Ressourcen zuzugreifen, um Aktionen mit Empfangsregeln auszuführen.

Wenn Sie eine Domänenidentität erstellen und verifizieren, veröffentlichen Sie Datensätze in Ihren DNS-Einstellungen, um den Überprüfungsprozess abzuschließen. Dies allein reicht jedoch nicht aus, um den E-Mail-Empfang zu verwenden. Speziell für den E-Mail-Empfang ist es auch erforderlich, einen MX-Eintrag für die Angabe einer benutzerdefinierten E-Mail-Domäne zu veröffentlichen. Dieser Eintrag wird in den DNS-Einstellungen Ihrer Domain verwendet, damit SES E-Mails für Ihre Domain erhalten kann. Das Erteilen von Berechtigungen ist erforderlich, da die Aktionen, die Sie in Ihren Empfangsregeln auswählen, nur funktionieren, wenn Amazon SES die Erlaubnis hat, den jeweiligen AWS Service zu nutzen, der für diese Aktionen erforderlich ist.

Diese drei Voraussetzungen, die zum Empfangen von E-Mails erforderlich sind, werden in den folgenden Themen beschrieben:

- Verifizieren Ihrer Domäne für den Amazon-SES-E-Mail-Empfang
- Veröffentlichen eines MX-Datensatzes für den Amazon-SES-E-Mail-Empfang
- Erteilen von Berechtigungen an Amazon SES für den E-Mail-Empfang

Verifizieren Ihrer Domäne für den Amazon-SES-E-Mail-Empfang

Wie bei allen Domänen, die Sie für das Senden und Empfangen von E-Mails mit Amazon SES verwenden möchten, müssen Sie zunächst nachweisen, dass Sie der Domänenbesitzer sind. Das Verifizierungsverfahren, das die Initiierung der Domänenverifizierung mit SES und die anschließende Veröffentlichung der DNS-Datensätze, entweder als CNAME oder TXT, auf Ihrem DNS-Anbieter umfasst, hängt davon ab, welche Verifizierungsmethode Sie verwenden.

Über die Konsole können Sie Ihre Domänen entweder mit Easy DKIM oder Bring Your Own DKIM (BYODKIM) verifizieren und ihre DNS-Datensätze ganz einfach kopieren, um sie bei Ihrem DNS-Anbieter zu veröffentlichen. Wie das geht, wird in Erstellen einer Domänenidentität erläutert. Optional können Sie entweder den SES `VerifyDomainDkim`oder verwenden `VerifyDomainIdentity` APIs.

Sie können ganz einfach überprüfen, ob Ihre Domain oder E-Mail-Adresse verifiziert ist, indem Sie ihren Status in der Tabelle Verifizierte Identitäten in der SES-Konsole überprüfen oder entweder SES `GetIdentityVerificationAttributes`oder `GetEmailIdentity` APIsverwenden.

Veröffentlichen eines MX-Datensatzes für den Amazon-SES-E-Mail-Empfang

Ein Mail Exchanger-Datensatz (MX-Datensatz#) ist eine Konfiguration, die angibt, welche Mailserver E-Mails annehmen können, die an Ihre Domäne gesendet werden.

Wenn Ihre eingehenden E-Mails über Amazon SES verwaltet werden sollen, müssen Sie zur DNS-Konfiguration Ihrer Domäne einen MX-Datensatz hinzufügen. Der MX-Eintrag, den Sie erstellen, bezieht sich auf den Endpunkt, der E-Mails für die AWS Region empfängt, in der Sie Amazon SES verwenden. Der Endpunkt für die Region USA West (Oregon) ist z.B. inbound-smtp.us-west-2.amazonaws.com. Eine vollständige Liste der Endpunkte finden Sie unter SES-Regionen und Endpunkte.

> **Note**
>
> Die Endpunkte, die E-Mails in Amazon SES empfangen, sind keine IMAP- oder POP3 E-Mail-Server. Sie können diese nicht URLs als Posteingangsserver in E-Mail-Clients verwenden. Wenn Sie eine Lösung benötigen, mit der Sie mithilfe eines E-Mail-Clients sowohl E-Mails senden als auch empfangen können, sollten Sie Amazon in Betracht ziehen WorkMail.

Das folgende Verfahren enthält allgemeine Schritte zum Erstellen eines MX-Datensatzes. Die spezifischen Verfahren zum Erstellen eines MX-Eintrags hängen von Ihrem DNS- oder Hosting-Anbieter ab. Weitere Informationen über das Hinzufügen eines MX-Datensatzes zur DNS-Konfiguration für Ihre Domäne finden Sie in der Dokumentation Ihres Anbieters.

> **Note**

So fügen Sie einen MX-Datensatz zur DNS-Konfiguration für Ihre Domäne hinzu:

1. (Voraussetzung) Um diese Verfahren abzuschließen, müssen Sie die DNS-Einträge für Ihre Domain ändern. Wenn Sie nicht auf die DNS-Einträge zugreifen können oder sich damit nicht wohlfühlen, wenden Sie sich an Ihren Systemadministrator, um Unterstützung zu erhalten.
2. Melden Sie sich bei der Managementkonsole für Ihren DNS-Anbieter an.
3. Erstellen Sie einen neuen MX-Datensatz.
4. Geben Sie für den Namen des MX-Datensatzes Ihre Domäne ein. Wenn Sie beispielsweise möchten, dass Amazon SES E-Mails verwaltet, die an die Domäne example.com gesendet werden, geben Sie Folgendes ein:

   ```
   example.com.
   ```

   > **Note**
   >
   > Abhängig von Ihrem DNS-Anbieter: 1) Das Trailing `.` am Ende der Domainendung ist möglicherweise nicht erforderlich. 2) Das Feld Name kann als Host -, Domain- oder Mail-Domain bezeichnet werden.

5. Wählen Sie für Type (Typ) die Option MX aus.

   > **Note**
   >
   > Bei einigen DNS-Anbietern wird das Feld Type (Typ) als Record Type (Datensatztyp) oder so ähnlich bezeichnet.

6. Geben Sie für Value (Wert) Folgendes ein:

```
10 inbound-smtp.region.amazonaws.com
```

Ersetzen Sie es im vorherigen Beispiel *region* durch die Adresse des Endpunkts, der E-Mails für die AWS Region empfängt, die Sie mit Amazon SES verwenden. Wenn Sie beispielsweise die Region USA Ost (Nord-Virginia) verwenden, *region* ersetzen Sie durch`us-east-1`. Eine Liste aller Endpunkte für den E-Mail-Empfang finden Sie unter SES-Regionen und Endpunkte.

> **Note**
>
> Die Verwaltungskonsolen einiger DNS-Anbieter enthalten separate Felder für Value (Wert) und Priority (Priorität) des Datensatzes. Wenn dies bei Ihrem DNS-Anbieter der Fall ist, geben Sie `10` als Wert für Priority (Priorität) und die URL des Endpunkts für den Posteingang für Value (Wert) ein.

> **Important**
>
> Das spezifische Verfahren für das Erstellen eines MX-Datensatzes hängt von Ihrem DNS- oder Hosting-Anbieter ab. Informationen zum Hinzufügen eines MX-Eintrags zur DNS-Konfiguration für Ihre Domain erhalten Sie in der Dokumentation Ihres Anbieters oder kontaktieren Sie ihn.

Anweisungen zum Erstellen von MX-Datensätzen für verschiedene Anbieter

Das Verfahren zum Erstellen eines MX-Datensatzes für Ihre Domäne hängt davon ab, welchen DNS-Anbieter Sie verwenden. Dieser Abschnitt enthält Links zur Dokumentation für mehrere gängige DNS-Anbieter. Diese Liste ist keine vollständige Anbieterliste. Wenn Ihr Anbieter unten nicht aufgeführt ist, können Sie ihn wahrscheinlich weiterhin mit Amazon SES verwenden. Die Aufnahme in diese Liste ist keine Empfehlung oder Empfehlung für die Produkte oder Dienstleistungen eines Unternehmens.

Name des DNS/Hosting-Anbieters	Link zur Dokumentation
Amazon Route 53	Erstellen von Datensätzen mit der Amazon-Route-53-Konsole

Name des DNS/Hosting-Anbieters	Link zur Dokumentation
GoDaddy	Einen MX-Datensatz hinzufügen (externer Link)
DreamHost	Wie ändere ich meine MX-Datensätze? (externer Link)
Cloudflare	Einrichten von E-Mail-Datensätzen (externer Link)
HostGator	Ändern von MX-Datensätzen – Windows (externer Link)
Namecheap	Wie kann ich die für den Mail-Service benötigten MX-Datensätze einrichten? (externer Link)
Names.co.uk	Ändern der DNS-Einstellungen Ihrer Domäne (externer Link)
Wix	Hinzufügen oder Aktualisieren von MX-Datensätzen in Ihrem Wix-Konto (externer Link)

Erteilen von Berechtigungen an Amazon SES für den E-Mail-Empfang

Für einige Aufgaben, die Sie ausführen können, wenn Sie E-Mails in SES empfangen, z. B. das Senden von E-Mails an einen Amazon Simple Storage Service (Amazon S3) -Bucket oder das Aufrufen einer AWS Lambda Funktion, sind spezielle Berechtigungen erforderlich. Dieser Abschnitt zeigt Richtlinienbeispiele für mehrere allgemeine Anwendungsfälle.

Themen in diesem Abschnitt:

- Einrichtung von IAM-Rollenberechtigungen für die Bucket-Aktion „An S3 liefern“
- Erteilen Sie SES die Erlaubnis, in einen S3-Bucket zu schreiben
- Erteilen Sie SES die Erlaubnis, Ihren AWS KMS Schlüssel zu verwenden
- Erteilen Sie SES die Erlaubnis, eine Funktion aufzurufen AWS Lambda
- Erteilen Sie SES die Erlaubnis, in einem Amazon SNS SNS-Thema zu veröffentlichen, das zu einem anderen AWS Konto gehört

Einrichtung von IAM-Rollenberechtigungen für die Bucket-Aktion „An S3 liefern“

Die folgenden Punkte gelten für diese IAM-Rolle:

- Sie kann nur für Aktion „An S3-Bucket liefern“ verwendet werden.
- Es muss verwendet werden, wenn Sie in einen S3-Bucket schreiben möchten, der in einer Region existiert, in der SES nicht the section called “Empfangen von E-Mails” verfügbar ist.

Wenn Sie in einen S3-Bucket schreiben möchten, können Sie eine IAM-Rolle mit Berechtigungen für den Zugriff auf die entsprechenden Ressourcen bereitstellen. Aktion „An S3-Bucket liefern“ Sie müssten SES außerdem die Erlaubnis erteilen, diese Rolle zu übernehmen, um die Aktion über eine IAM-Vertrauensrichtlinie auszuführen, wie im nächsten Abschnitt beschrieben.

Diese Berechtigungsrichtlinie muss in den integrierten Richtlinieneditor der IAM-Rolle eingefügt werden. Lesen Aktion „An S3-Bucket liefern“ und befolgen Sie die im IAM-Rollenelement angegebenen Schritte. (Das folgende Beispiel beinhaltet auch optionale Berechtigungen für den Fall, dass Sie eine SNS-Themenbenachrichtigung oder einen vom Kunden verwalteten Schlüssel in der S3-Aktion verwenden möchten.)

> **Note**
>
> - Sie haben die Möglichkeit, die S3-Aktion ohne Angabe einer IAM-Rolle einzurichten, indem Sie nur den SES-Dienst in der S3-Bucket-Richtlinie zulassen, wie hier gezeigt. the section called “Erteilen Sie SES die Erlaubnis, in einen S3-Bucket zu schreiben” Dies funktioniert auch für kontoübergreifende Szenarien.
> - Wenn Sie eine IAM-Rolle für die S3-Aktion angeben, nimmt SES diese Rolle für den Vorgang 'PutObject' an, und die hier angegebenen IAM-Berechtigungen reichen für dieselbe Kontonutzung aus. Für die kontoübergreifende Nutzung benötigen Sie jedoch eine zusätzliche Bucket-Richtlinie, die es der IAM-Rolle ermöglicht, im Bucket 'PutObject' zu stehen. Dies wird dadurch spezifiziert, dass der Bucket-Besitzer kontoübergreifende Bucket-Berechtigungen erteilt, wie unter Bucket-Besitzer, der kontoübergreifende Bucket-Berechtigungen erteilt, erklärt wird.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": "sns:Publish",
            "Resource": "arn:aws:sns:us-east-1:111122223333:my-topic"
        },
        {
            "Sid": "KMSAccess",
            "Effect": "Allow",
            "Action": "kms:GenerateDataKey*",
            "Resource": "arn:aws:kms:us-east-1::111122223333:key/key-id"
        }
    ]
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- *amzn-s3-demo-bucket*Ersetzen Sie es durch den Namen des S3-Buckets, in den Sie schreiben möchten.
- *region*Ersetzen Sie durch den AWS-Region Ort, an dem Sie die Empfangsregel erstellt haben.
- Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID.
- *my-topic*Ersetzen Sie es durch den Namen des SNS-Themas, zu dem Sie Benachrichtigungen veröffentlichen möchten.
- *key-id*Ersetzen Sie es durch die ID Ihres KMS-Schlüssels.

Vertrauensrichtlinie für die IAM-Rolle S3-Aktion

Die folgende Vertrauensrichtlinie sollte zu den Vertrauensbeziehungen der IAM-Rolle hinzugefügt werden, damit SES diese Rolle übernehmen kann.

> **Note**
>
> Das manuelle Hinzufügen dieser Vertrauensrichtlinie ist nur erforderlich, wenn Sie Ihre IAM-Rolle nicht mithilfe der im IAM-Rollenelement des Workflows angegebenen Schritte von der SES-Konsole aus erstellt haben. Aktion „An S3-Bucket liefern“ Wenn Sie die IAM-Rolle von der Konsole aus erstellen, wird diese Vertrauensrichtlinie automatisch generiert und auf die Rolle angewendet, sodass dieser Schritt nicht erforderlich ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESAssume",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                  "AWS:SourceAccount":"111122223333",
                  "AWS:SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-set/rule_set_name:receipt-rule/receipt_rule_name"
                }
            }
        }
    ]
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- Ersetzen Sie sie *region* durch die AWS-Region Stelle, an der Sie die Empfangsregel erstellt haben.
- Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID.

- *rule_set_name*Ersetzen Sie es durch den Namen des Regelsatzes, der die Empfangsregel enthält, die die S3-Bucket-Aktion „An Amazon liefern“ enthält.
- *receipt_rule_name*Ersetzen Sie es durch den Namen der Empfangsregel, die die Bucket-Aktion „An Amazon S3 liefern“ enthält.

Erteilen Sie SES die Erlaubnis, in einen S3-Bucket zu schreiben

Wenn Sie die folgende Richtlinie auf einen S3-Bucket anwenden, erteilt sie SES die Erlaubnis, in diesen Bucket zu schreiben, solange dieser in einer Region existiert, in der SES-E-Mail-Empfang verfügbar ist. Wenn Sie in einen Bucket außerhalb einer E-Mail-Empfangsregion schreiben möchten, finden Sie unter. Einrichtung von IAM-Rollenberechtigungen für die Bucket-Aktion „An S3 liefern“ Weitere Informationen zum Erstellen von Empfangsregeln, die eingehende E-Mails an Amazon S3 übertragen, finden Sie unter Aktion „An S3-Bucket liefern“.

Weitere Informationen zu Bucket-Richtlinien für Amazon S3 finden Sie unter Verwenden von Bucket-Richtlinien und Benutzerrichtlinien im Amazon Simple Storage Service-Entwicklerleitfaden.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AllowSESPuts",
      "Effect":"Allow",
      "Principal":{
        "Service":"ses.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition":{
        "StringEquals":{
          "AWS:SourceAccount":"111122223333",
          "AWS:SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
    }
  ]
```

```
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- *amzn-s3-demo-bucket*Ersetzen Sie es durch den Namen des S3-Buckets, in den Sie schreiben möchten.
- *region*Ersetzen Sie es durch die AWS Region, in der Sie die Empfangsregel erstellt haben.
- Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID.
- *rule_set_name*Ersetzen Sie es durch den Namen des Regelsatzes, der die Empfangsregel enthält, die die S3-Bucket-Aktion „An Amazon liefern“ enthält.
- *receipt_rule_name*Ersetzen Sie es durch den Namen der Empfangsregel, die die Bucket-Aktion „An Amazon S3 liefern“ enthält.

Erteilen Sie SES die Erlaubnis, Ihren AWS KMS Schlüssel zu verwenden

Damit SES Ihre E-Mails verschlüsseln kann, muss es berechtigt sein, den AWS KMS Schlüssel zu verwenden, den Sie bei der Einrichtung Ihrer Empfangsregel angegeben haben. Sie können entweder den Standardhauptschlüssel (aws/ses) in Ihrem Konto oder einen benutzerdefinierten Hauptschlüssel, den Sie erstellen, verwenden. Wenn Sie den Standard-KMS-Schlüssel verwenden, müssen Sie keine zusätzlichen Schritte ausführen, um SES die Erlaubnis zur Verwendung zu erteilen. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, müssen Sie SES die Erlaubnis zur Verwendung dieses Schlüssels erteilen, indem Sie der Richtlinie für den Schlüssel eine Erklärung hinzufügen.

Verwenden Sie die folgende Grundsatzerklärung als wichtigste Richtlinie, damit SES Ihren vom Kunden verwalteten Schlüssel verwenden kann, wenn es E-Mails auf Ihrer Domain empfängt.

```
{
  "Sid": "AllowSESToEncryptMessagesBelongingToThisAccount",
  "Effect": "Allow",
  "Principal": {
    "Service":"ses.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition":{
```

```
        "StringEquals":{
          "AWS:SourceAccount":"111122223333",
          "AWS:SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- *region*Ersetzen Sie es durch die AWS Region, in der Sie die Empfangsregel erstellt haben.
- Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID.
- *rule_set_name*Ersetzen Sie es durch den Namen des Regelsatzes, der die Empfangsregel enthält, die Sie dem E-Mail-Empfang zugeordnet haben.
- *receipt_rule_name*Ersetzen Sie es durch den Namen der Empfangsregel, die Sie dem E-Mail-Empfang zugeordnet haben.

Wenn Sie das Senden verschlüsselter Nachrichten an einen S3-Bucket mit aktivierter serverseitiger Verschlüsselung verwenden AWS KMS , müssen Sie die Richtlinienaktion hinzufügen. `"kms:Decrypt"` Im obigen Beispiel würde das Hinzufügen dieser Aktion zu Ihrer Richtlinie wie folgt aussehen:

```
{
  "Sid": "AllowSESToEncryptMessagesBelongingToThisAccount",
  "Effect": "Allow",
  "Principal": {
    "Service":"ses.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition":{
        "StringEquals":{
          "AWS:SourceAccount":"111122223333",
          "AWS:SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
```

```
}
```

Weitere Informationen zum Anhängen von Richtlinien an AWS KMS Schlüssel finden Sie unter Verwenden von Schlüsselrichtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Erteilen Sie SES die Erlaubnis, eine Funktion aufzurufen AWS Lambda

Damit SES eine AWS Lambda Funktion aufrufen kann, können Sie die Funktion auswählen, wenn Sie eine Empfangsregel in der SES-Konsole erstellen. Wenn Sie dies tun, fügt SES der Funktion automatisch die erforderlichen Berechtigungen hinzu.

Sie können aber auch die `AddPermission`-Operation in der AWS Lambda -API verwenden, um eine Richtlinie an eine Funktion anzufügen. Der folgende `AddPermission` API-Aufruf erteilt SES die Erlaubnis, Ihre Lambda-Funktion aufzurufen. Weitere Informationen zum Anfügen von Richtlinien an Lambda-Funktionen finden Sie unter AWS Lambda -Berechtigungen im AWS Lambda -Entwicklerleitfaden.

```
{
  "Action": "lambda:InvokeFunction",
  "Principal": "ses.amazonaws.com",
  "SourceAccount": "111122223333",
  "SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-set/rule_set_name:receipt-
rule/receipt_rule_name",
  "StatementId": "GiveSESPermissionToInvokeFunction"
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- Ersetzen Sie es *region* durch die AWS Region, in der Sie die Empfangsregel erstellt haben.
- Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID.
- *rule_set_name*Ersetzen Sie durch den Namen des Regelsatzes, der die Empfangsregel enthält, in der Sie Ihre Lambda-Funktion erstellt haben.
- *receipt_rule_name*Ersetzen Sie durch den Namen der Empfangsregel, die Ihre Lambda-Funktion enthält.

Erteilen Sie SES die Erlaubnis, in einem Amazon SNS SNS-Thema zu veröffentlichen, das zu einem anderen AWS Konto gehört

Um Benachrichtigungen zu einem Thema in einem separaten AWS Konto zu veröffentlichen, müssen Sie eine Richtlinie an das Amazon SNS SNS-Thema anhängen. Das SNS-Thema muss sich in derselben Region wie die Domänen- und Empfangsregelsätze befinden.

Die folgende Richtlinie erteilt SES die Erlaubnis, Beiträge zu einem Amazon SNS SNS-Thema in einem separaten AWS Konto zu veröffentlichen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111122223333:topic_name",
            "Condition": {
                "StringEquals": {
                "AWS:SourceAccount": "444455556666",
                "AWS:SourceArn": "arn:aws:ses:us-east-1:777788889999:receipt-
rule-set/rule_set_name:receipt-rule/rule_name"
                }
            }
        }
    ]
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- *topic_region*Ersetzen Sie es durch AWS-Region das, in dem das Amazon SNS SNS-Thema erstellt wurde.
- *sns_topic_account_id*Ersetzen Sie es durch die ID des AWS Kontos, dem das Amazon SNS SNS-Thema gehört.

- *topic_name*Ersetzen Sie es durch den Namen des Amazon SNS SNS-Themas, zu dem Sie Benachrichtigungen veröffentlichen möchten.
- *aws_account_id*Ersetzen Sie es durch die ID des AWS Kontos, das für den Empfang von E-Mails konfiguriert ist.
- *receipt_region*Ersetzen Sie durch den AWS-Region Ort, an dem Sie die Empfangsregel erstellt haben.
- *rule_set_name*Ersetzen Sie es durch den Namen des Regelsatzes, der die Empfangsregel enthält, mit der Sie Ihre Themenaktion „In Amazon SNS veröffentlichen“ erstellt haben.
- *receipt_rule_name*Ersetzen Sie es durch den Namen der Empfangsregel, die die Themenaktion „In Amazon SNS veröffentlichen“ enthält.

Wenn Ihr Amazon SNS SNS-Thema AWS KMS serverseitige Verschlüsselung verwendet, müssen Sie der AWS KMS Schlüsselrichtlinie Berechtigungen hinzufügen. Sie können Berechtigungen hinzufügen, indem Sie die folgende Richtlinie an die Schlüsselrichtlinie anhängen: AWS KMS

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESToUseKMSKey",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon SES E-Mail-Empfangskonsole — exemplarische Vorgehensweisen

In diesem Abschnitt werden die Assistenten für die E-Mail-Empfangskonsole beschrieben, die zum Konfigurieren von -Empfangsregeln und IP-Adressenfilter, um Ihren E-Mail-Empfang zu verwalten. Bevor Sie die Konsolenassistenten verwenden, ist es wichtig, dass Sie sowohlE-Mail-Empfangskonzepte & Anwendungsfälle, um die Konzepte zu verstehen, wie der E-Mail-Empfang funktioniert und mit Einrichten des E-Mail-Empfangs in stellen Sie sicher, dass Sie die Setup-Voraussetzungen erfüllt haben.

Die Konsolenassistenten zum Konfigurieren von Empfangsregeln und IP-Adressfiltern werden im Folgenden erläutert:

- Exemplarische Vorgehensweise in der Konsole für Zahlungsregeln erstellen
- Exemplarische Vorgehensweise bei der Konfiguration von IP-Adressenfiltern

Exemplarische Vorgehensweise in der Konsole für Zahlungsregeln erstellen

Dieser Abschnitt führt Sie durch das Erstellen und Definieren von Zahlungsregeln mit der Amazon SES Konsole. Die wichtigsten Punkte für das Verständnis der Funktionsweise von erstellten Regeln sind:

- In Rule sets (Regelsätze) eine geordnete Reihe von Zahlungsregeln enthalten; Receipt rules (Empfangsregeln) enthalten eine geordnete Reihe von Aktionen.
- Zahlungsregeln geben Amazon SES an, wie eingehende E-Mails verarbeitet werden sollen, indem eine geordnete Liste von Aktionen ausgeführt wird, die Sie angeben.
- Diese geordnete Liste von Aktionen kann optional davon abhängig gemacht werden, dass zuerst eine Empfängerbedingung erfüllt wird. Wenn nicht angegeben, werden die Aktionen auf alle Identitäten angewendet, die zu Ihren verifizierten Domains gehören.
- Wareneingangsregeln werden in einem Container, der als Regelsatz bezeichnet wird, erstellt und definiert. Während Sie mehrere Regelsätze erstellen können, kann jeweils nur eines aktiv sein.
- Wareneingangsregeln innerhalb des aktiven Regelsatzes werden in der von Ihnen angegebenen Reihenfolge ausgeführt.
- Bevor Sie die Empfangsregeln erstellen, müssen Sie zunächst eine-Regelsatzum sie einzudämmen.

Verwenden der `CreateReceiptRuleSet`-API – Verwenden Sie die -API zum Erstellen eines leeren Empfangsregelsatzes, wie in der Referenz zur Amazon Simple Email Service API Reference beschrieben. Anschließend können Sie mithilfe der Amazon-SES-Konsole oder der `CreateReceiptRule`-API Empfangsregeln hinzufügen.

Bevor Sie mit der exemplarischen Vorgehensweise fortfahren, stellen Sie sicher, dass Sie alle erforderlichen Voraussetzungen erfüllt haben, die für die Verwendung des empfängerbasierten E-Mail-Empfangs erforderlich sind.

Voraussetzungen

Die folgenden Voraussetzungen müssen erfüllt sein, bevor Sie mit Empfangsregeln die empfängerbasierte E-Mail-Steuerung einrichten:

1. Stellen Sie sicher, dass sich Ihr Endpunkt an einem AWS-Region Ort befindet, an dem Amazon SES den E-Mail-Empfang unterstützt. In der Tabelle mit den E-Mail-Empfangsendpunkten in der Allgemeine AWS-Referenz Tabelle sind die E-Mail-Empfangsendpunkte für alle Bereiche aufgeführt, AWS-Regionen in denen SES den E-Mail-Empfang unterstützt.
2. Sie müssen zuerstErstellen und Überprüfen einer Domänen-IdentitätAmazon SES.
3. Als Nächstes müssen Sie angeben, welche Mail-Server E-Mails für Ihre Domain akzeptieren können, indem SieVeröffentlichen eines MX-Datensatzesauf die DNS-Einstellungen Ihrer Domäne. (Der MX-Eintrag sollte sich auf den Amazon SES-Endpunkt beziehen, der E-Mails für die AWS Region empfängt, in der Sie Amazon SES verwenden.)
4. Schließlich müssen Sie Amazon SES die Erlaubnis erteilen, auf andere AWS Ressourcen zuzugreifen, um Empfangsregelaktionen ausführen zu können.

Erstellen von RegelSets und Zahlungsregeln

Diese exemplarische Vorgehensweise beginnt, indem Sie zuerst einen Regelsatz erstellen, der Ihre Regeln enthält und in die den Assistenten Create rule (Regel erstellen) vorahgeht, um Ihre Zahlungsregeln zu erstellen, zu definieren und anzuordnen. Der Assistent enthält vier Bildschirme zum Definieren von Regeleinstellungen, Hinzufügen von Empfängerbedingungen, Hinzufügen von Aktionen und zum Überprüfen aller Einstellungen.

So erstellen Sie eine Empfangsregel mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.

2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) die Option Email Receiving (Empfangen von E-Mails) aus.

> **Note**
>
> Der E-Mail-Empfang ist im linken Navigationsbereich der SES-Konsole nicht sichtbar, wenn sich Ihr Konto in einer AWS-Region befindet, in der SES den E-Mail-Empfang nicht unterstützt. Siehe den ersten Punkt unter the section called “Voraussetzungen”.

3. Wählen Sie auf der Registerkarte Receipt rule sets (Empfangsregelsätze) im Bereich Email receiving (Empfangen von E-Mails) die Option Create rule set (Regelsatz erstellen) aus.
4. Geben Sie einen eindeutigen Namen für Ihren Regelsatz ein und wählen Sie Create rule set (Regelsatz erstellen) aus.
5. Wählen Sie Create rule (Regel erstellen) und dies öffnet den Assistenten Create rule (Regel erstellen).
6. Geben Sie auf der Seite Define rule settings (Definieren von Regeleinstellungen), unter Receipt rule details (Details zur Empfangsregelsatz) einen Rule name (Regelnamen) ein.
7. Für Status, löschen Sie nur dieKontrollbox Enabled (Aktiviert), wenn Sie nicht möchten, dass Amazon SES diese Regel nach der Erstellung ausführt. Andernfalls lassen Sie diese Option aktiviert.
8. (Optional) Unter Security and protection options (Sicherheits- und Schutzoptionen), für Transport Layer Security (TLS), select Required (Erforderlich), wenn Amazon SES eingehende Nachrichten ablehnt, die nicht über eine sichere Verbindung gesendet werden.
9. (Optional) Wenn Amazon SES eingehende E-Mails auf Spam und Viren überprüfen soll, wählen Sie für Spam and virus scanning (Spam und Virenprüfung) Enable (Aktivieren) aus.
10. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus, um mit dem nächsten Schritt fortzufahren.
11. (Optional) Verwenden Sie auf der Registerkarte Add recipient conditions (Empfängerbedingungen hinzufügen) das folgende Verfahren, um eine oder mehrere Empfängerbedingungen anzugeben. Sie können maximal 100 Empfänger pro Empfangsregel hinzufügen.

    a. Wählen Sie unter Recipient conditions (Empfängerbedingungen) Add new recipient condition (Neue Empfängerbedingung hinzufügen), um die Empfangsregel oder Domäne anzugeben, auf die Sie die Empfangsregel anwenden möchten. In der folgenden Tabelle wird die Adresse user@example.com verwendet, um zu zeigen, wie Empfänger angegeben werden.

Wenn Sie …	Den folgenden Empfänger angeben ...	Hinweise
Ordnen Sie eine bestimmte E-Mail-Adresse zu.	user@example.com	Es werden auch Varianten der Adresse zugeordnet, die Labels enthalten (z. B. user+123@example.com und user+xyz@example.com). Wenn Sie jedoch eine Adresse angeben, die einen Label enthält, wird nur diese bestimmte Adresse zugeordnet.
Ordnen Sie alle Adressen innerhalb einer Domäne zu, jedoch nicht diejenigen in den Subdomänen.	example.com	
Ordnen Sie alle Adressen innerhalb einer bestimmten Subdomäne zu, jedoch nicht diejenigen in der übergeordneten Domäne.	subdomain.example.com	
Ordnen Sie alle Adressen innerhalb aller Subdomänen zu, jedoch nicht diejenigen in der übergeordneten Domäne.	.example.com	Beachten Sie den Punkt (.) vor dem Domänennamen.
Ordnen Sie alle Adressen innerhalb einer Domäne und alle Adressen in allen Subdomänen zu.	example.com .example.com	Erstellen Sie zwei separate Empfänger: einen mit dem Domänennamen und einen mit einem Punkt gefolgt vom Domänennamen.

Wenn Sie …	Den folgenden Empfänger angeben ...	Hinweise
Zuordnen aller Empfänger in allen verifizierten Domänen	[Keine]	Lassen Sie das Empfänger feld leer.

> **Important**
>
> Wenn mehrere Amazon-SES-Konten E-Mails in einer gemeinsamen Domäne empfangen (z. B. wenn mehrere Teams im selben Unternehmen jeweils über separate Amazon-SES-Konten verfügen), verarbeitet Amazon SES alle passenden Empfangsregeln für jedes dieser Konten gleichzeitig. Dieses Verhalten kann dazu führen, dass ein Konto eine Unzustellbarkeitsnachricht generiert, während ein anderes Konto die E-Mail akzeptiert.
> Wir empfehlen die Koordination mit anderen Teams in Ihrer Organisation, die Amazon SES verwenden, um sicherzustellen, dass jedes Konto eindeutige Empfangsregeln verwendet und dass sich diese Regeln nicht überschneiden. In diesen Fällen empfiehlt es sich, Ihre Empfangsregeln nur für E-Mail-Adressen oder Subdomänen zu konfigurieren, die für Ihre Gruppe oder Ihr Team eindeutig sind.

b. Wiederholen Sie diesen Schritt für jede Empfängerbedingung, die Sie hinzufügen möchten. Wenn Sie alle Empfänger hinzugefügt haben, wählen Sie Next Step (Nächster Schritt) aus.

12. Führen Sie auf der Seite Add actions (Aktionen hinzufügen) die folgenden Schritte aus, um der Empfangsregel eine oder mehrere Aktionen hinzuzufügen.

    a. Öffnen Sie Add new action (Neue Aktion hinzufügen) und wählen Sie dann eine der folgenden Aktionen aus:

    - Add Header - Diese Aktion wird der empfangenen E-Mail ein benutzerdefinierter Header hinzugefügt.
    - Return Bounce Response- Diese Aktion lehnt die empfangene E-Mail mit einer Unzustellbarkeitsnachricht an den Sender ab.

- Aufrufen einer -Lambda-Funktion- Diese Aktion ruft Ihren Code über eine AWS Lambda-Funktion auf.
- Liefern an S3-Bucket- Diese Aktion speichert die empfangene E-Mail in einem Amazon Simple Storage Service (S3) -Bucket.
- Veröffentlichen in einem Amazon SNS-Thema.- Diese Aktion veröffentlicht die vollständige E-Mail in einem Amazon Simple Notification Service (SNS).
- Stopp-Regelsatz- Diese Aktion beendet die Auswertung des Empfangsregelsatzes.
- Integrieren Sie mit Amazon WorkMail- Diese Aktion ist in Amazon integriert WorkMail.

Weitere Informationen über alle diese Aktionen finden Sie im Aktionsoptionen.

b. Wiederholen Sie diesen Schritt für jede Aktion, die Sie definieren möchten. Wenn Sie mehrere Aktionen definiert haben, können Sie diese mithilfe der Aufwärts/Abwärtspfeile innerhalb der Aktionscontainer neu anordnen. Wählen Sie Next (Weiter) aus, um die Seite Review (Überprüfen) zu öffnen.

13. Überprüfen Sie auf der Seite Review (Überprüfen) die Einstellungen und Aktionen der Regel. Wenn Sie Änderungen vornehmen müssen, verwenden Sie die Option Edit (Bearbeiten) oder den Navigationsbereich auf der linken Seite des Fensters, direkt zu der Seite zu gelangen, die den zu bearbeitenden Inhalt enthält. Sie können optional die Reihenfolge der Aktionen ändern, die in der Tabelle Aktionen der Bewertungsseite aufgeführt sind, indem Sie die up/down Pfeile in der Spalte „Neu anordnen“ verwenden.
14. Wenn Sie bereit sind, fortzufahren, wählen Sie Create user (Benutzer erstellen) aus.
15. Wählen Sie auf der Bestätigungsseite für den Regelsatz die Option Set as active (Als aktiv festlegen) aus, wenn Sie den Regelsatz sofort erzwingen möchten.

Regeländerungen nach der Erstellung

Nachdem Sie einen Regelsatz erstellt haben, können Sie sowohl den Regelsatz als auch die darin enthaltenen Zahlungsregeln bearbeiten. Sie können nicht nur bearbeitet werden, sondern es gibt auch die Möglichkeit, entweder den Regelsatz oder seine Regeln zu duplizieren, damit neue schnell erstellt werden können. Die folgende Liste zeigt die verfügbaren Änderungen für das RegelSet und die Zahlungsregeln:

- Rule set (Regelsatz) wird mit Namen, Status und Erstellungsdatum aufgeführt. Änderungsoptionen für den Regelsatz sind:
  - Umschalttaste Als aktiv/inaktiv festlegen wechselt zwischen der Einstellung des Status.

  - Die Schaltfläche Duplicate (Duplikat) kopiert den Regelsatz. Sie werden aufgefordert, einen eindeutigen Namen anzugeben.
  - Die Schaltfläche Delete (Löschen) löscht den Regelsatz. Sie werden aufgefordert, diese unumkehrbare Aktion zu bestätigen.
- Receipt rules (Empfangsregeln) werden mit Namen, Status, Sicherheit und Reihenfolge aufgelistet. Änderungsoptionen für die Zahlungsregeln sind:
  - Pfeile nach oben/unten, um die Regelausführung innerhalb des Regelsatzes neu anzuordnen.
  - Die Schaltfläche Duplicate (Duplikat) erstellt eine Kopie der ausgewählten Regel. Sie werden aufgefordert, einen eindeutigen Namen anzugeben.
  - Die Schaltfläche Edit (Bearbeiten) öffnet die ausgewählte Regel, sodass alle Parameter wie Regeleinstellungen, Empfängerbedingungen und Aktionen bearbeitet werden können.
  - Die Schaltfläche Delete (Löschen) löscht die ausgewählte Regel. Sie werden aufgefordert, diese unumkehrbare Aktion zu bestätigen.
  - Die Schaltfläche Create rule (Regel erstellen) erlaubt Ihnen, eine neue Regel zu erstellen und dem aktuellen Regelsatz hinzuzufügen.

Aktionsoptionen

Jede Empfangsregel für den Amazon-SES-E-Mail-Empfang enthält eine geordnete Liste der Aktionen. In diesem Abschnitt werden die spezifischen Optionen für jeden Aktionstyp beschrieben.

Es stehen folgende Aktionstypen zur Verfügung:

- "Add Header"-Aktion
- Rücksprungantwort Aktion zurückgeben
- Aufrufen einer Lambda-Funktion
- Aktion „An S3-Bucket liefern“
- Veröffentlichen in einem Amazon SNS-Thema.
- Aktion „Regelsatz beenden“
- Mit Amazon WorkMail Action integrieren

"Add Header"-Aktion

Mit der Aktion Add Header (Header hinzufügen) wird der empfangenen E-Mail ein benutzerdefinierter Header hinzugefügt. Diese Aktion wird normalerweise nur in Kombination mit einer anderen Aktion verwendet. Diese Aktion umfasst die folgenden Optionen.

- Header name – Der Name des hinzuzufügenden Headers. Er muss zwischen 1 und 50 Zeichen lang sein und darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) und Bindestriche enthalten.
- Header value – Der Wert des hinzuzufügenden Headers. Er muss kleiner als 2048 Zeichen sein und darf kein Zeilenumbruchzeichen ("\r" oder"\n") enthalten.

Rücksprungantwort Aktion zurückgeben

Die Aktion Bounce (Unzustellbarkeit) lehnt die E-Mail mit einer Unzustellbarkeitsnachricht an den Sender ab und benachrichtigt Sie optional über Amazon SNS. Diese Aktion umfasst die folgenden Optionen.

- SMTP Reply Code – Der SMTP-Antwortcode gemäß RFC 5321.
- SMTP Status Code – Der erweiterte SMTP-Statuscode gemäß RFC 3463.
- Message – Lesbarer Text für die Unzustellbarkeits-E-Mail.
- Reply Sender – Die E-Mail-Adresse des Senders der unzustellbaren E-Mail. Dies ist die Adresse, von der die Unzustellbarkeits-E-Mail gesendet wird. Sie muss für Amazon SES verifiziert werden.

> **Note**
>
> Bounce-Nachrichten werden nicht über Ihre benutzerdefinierte MAIL FROM-Domain gesendet, sondern intern von SES generiert und ausschließlich mit der `amazonses.com` DKIM-Signatur signiert. Um das Problem zu umgehen, verwenden Sie die Option „Absender antworten“, um eine E-Mail-Adresse für Ihre Bounce-Nachrichten festzulegen. Weitere Informationen finden Sie in diesem AWS re:Post Artikel.

- SNS Topic – Der Name oder ARN des Amazon SNS-Themas, der optional benachrichtigt werden soll, wenn eine Unzustellbarkeits-E-Mail gesendet wird. Ein Beispiel für einen Amazon SNS SNS-Themen-ARN ist arn:aws:sns:us-east - 1:123456789012:. MyTopic Sie können ein Amazon-SNS-Thema auch beim Einrichten Ihrer Aktion erstellen, indem Sie Create SNS Topic (SNS-Thema erstellen) auswählen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf Ihre Amazon-SNS-Themen im Amazon Simple Notification Service-Entwicklerleitfaden.

> **Note**
>
> Das von Ihnen Amazon SNS SNS-Thema muss sich in derselben AWS Region befinden wie der Amazon SES SES-Endpunkt, den Sie für den E-Mail-Empfang verwenden.

Sie können Ihre eigenen Werte für diese Felder eingeben oder eine Vorlage auswählen, mit der die Felder "SMTP Reply Code", "SMTP Status Code" und "Message" mit Werten ausgefüllt werden, die auf der Ursache der Unzustellbarkeit beruhen. Die folgenden Vorlagen sind verfügbar:

- Mailbox Does Not Exist – SMTP Reply Code = 550, SMTP Status Code = 5.1.1
- Message Too Large – SMTP Reply Code = 552, SMTP Status Code = 5.3.4
- Mailbox Full – SMTP Reply Code = 552, SMTP Status Code = 5.2.2
- Message Content Rejected – SMTP Reply Code = 500, SMTP Status Code = 5.6.1
- Unknown Failure – SMTP Reply Code = 554, SMTP Status Code = 5.0.0
- Temporary Failure – SMTP Reply Code = 450, SMTP Status Code = 4.0.0

Zusätzliche Unzustellbarkeitscodes, die Sie nutzen können, indem Sie benutzerdefinierte Werte in die Felder eingeben, finden Sie in RFC 3463.

Aufrufen einer Lambda-Funktion

Die Lambda-Aktion ruft Ihren Code über eine Lambda-Funktion auf und benachrichtigt Sie optional über Amazon SNS. Diese Aktion umfasst die folgenden Optionen und Anforderungen.

Optionen

- Lambda-Funktion – ARN der Lambda-Funktion. Ein Beispiel für einen Lambda-Funktions-ARN ist arn:aws:lambda:us-east-1:account-id:function:. MyFunction
- Invocation type – Der Aufruftyp der Lambda-Funktion. Ein Aufruftyp von bedeutet, dass die Ausführung der Funktion zu einer sofortigen Antwort führt. RequestResponse Eine Aufruftyp Event (Ereignis) bedeutet, dass die Funktion asynchron aufgerufen wird. Wir empfehlen, den Aufruftyp Event (Ereignis) zu verwenden, es sei denn, für Ihren Anwendungsfall ist die synchrone Ausführung notwendig.

  Für den Aufruf von RequestResponse gibt es eine Zeitverzögerung von 30 Sekunden.

Weitere Informationen finden Sie unter Aufrufen von Lambda mit Step Functions im AWS Lambda - Entwicklerhandbuch.

- SNS-Thema – Der Name oder ARN des Amazon-SNS-Themas, das benachrichtigt werden soll, wenn die angegebene Lambda-Funktion ausgelöst wird. Ein Beispiel für einen Amazon SNS SNS-Themen-ARN ist arn:aws:sns:us-east - 1:123456789012:. MyTopic Weitere Informationen finden Sie unter Amazon SNS-Thema anlegen im Amazon Simple Notification Service-Entwicklerhandbuch.

Voraussetzungen

- Die Lambda-Funktion, die Sie auswählen, muss sich in derselben AWS Region befinden wie der Amazon SES SES-Endpunkt, den Sie für den Empfang von E-Mails verwenden.
- Das von Ihnen Amazon SNS SNS-Thema muss sich in derselben AWS Region befinden wie der Amazon SES SES-Endpunkt, den Sie für den E-Mail-Empfang verwenden.

Schreiben Ihrer Lambda-Funktion

Zum Verarbeiten Ihrer E-Mail kann Ihre Lambda-Funktion asynchron aufgerufen werden (d. h. mit dem `Event`-Aufruftyp). Das an Ihre Lambda-Funktion übergebene "Event"-Objekt enthält Metadaten zum eingehenden E-Mail-Ereignis. Sie können auch die Metadaten für den Zugriff auf den Nachrichteninhalt aus Ihrem Amazon-S3-Bucket verwenden.

Wenn Sie den Nachrichtenfluss wirklich kontrollieren möchten, muss Ihre Lambda-Funktion synchron aufgerufen werden (d. h. mit dem `RequestResponse`-Aufruftyp) und Ihre Lambda-Funktion muss die `callback` Methode mit zwei Argumenten aufrufen: Das erste Argument lautet `null` und das zweite ist eine `disposition`-Eigenschaft, die auf `STOP_RULE`, `STOP_RULE_SET` oder `CONTINUE` eingestellt ist. Wenn das zweite Argument `null` ist oder keine gültige `disposition`-Eigenschaft besitzt, wird der Nachrichtenfluss fortgesetzt und weitere Aktionen und Regeln werden verarbeitet. Dies entspricht dem Ablauf von `CONTINUE`.

Sie können beispielsweise den Empfangsregelsatz stoppen, indem Sie die folgende Zeile an das Ende des Lambda-Funktionscodes setzen:

```
callback( null, { "disposition" : "STOP_RULE_SET" });
```

AWS Lambda Codebeispiele finden Sie unterBeispiele für Lambda-Funktionen. Beispiele für allgemeine Anwendungsfälle finden Sie unter Beispielanwendungsfälle.

Eingabeformat

Amazon SES übergibt Informationen an die Lambda Funktion im JSON-Format. Das Objekt auf oberster Ebene enthält ein `Records`-Array, das mit Eigenschaften `eventSource`, `eventVersion` und `ses` gefüllt ist. Das `ses`-Objekt enthält `receipt`- und `mail`-Objekte, die das gleiche Format wie die in Benachrichtigungsinhalte beschriebenen Amazon-SNS-Benachrichtigungen aufweisen.

Die Daten, die Amazon SES an Lambda übergibt, enthalten Metadaten zur Nachricht sowie mehrere E-Mail-Header. Sie enthalten jedoch nicht den Text der Nachricht.

Im Folgenden finden Sie eine allgemeine Übersicht über die Struktur der Eingabe, die Amazon SES für die Lambda-Funktion bereitstellt.

```
{
   "Records": [
      {
        "eventSource": "aws:ses",
        "eventVersion": "1.0",
        "ses": {
           "receipt": {
               <same contents as SNS notification>
            },
           "mail": {
               <same contents as SNS notification>
           }
         }
     }
   ]
}
```

Rückgabewerte

Ihre Lambda-Funktion kann den Nachrichtenfluss kontrollieren, indem einer der folgenden Werte zurückgegeben wird:

- `STOP_RULE` – Es werden keine weiteren Aktionen in der aktuellen Empfangsregel, jedoch weitere Empfangsregeln verarbeitet.
- `STOP_RULE_SET` – Es werden keine weiteren Aktionen oder Empfangsregeln verarbeitet.
- `CONTINUE` oder ein anderer ungültiger Wert – Das bedeutet, dass weitere Aktionen und Empfangsregeln verarbeitet werden können.

Die folgenden Themen behandeln Beispiele für eingehende E-Mail-Ereignisse, Beispiele für allgemeine Anwendungsfälle und AWS Lambda Codebeispiele:

- Beispielanwendungsfälle
- Beispiele für Lambda-Funktionen

Beispielanwendungsfälle

Die folgenden Beispiele beschreiben einige Regeln, die Sie für die Verwendung der Lambda-Funktionsergebnisse zum Kontrollieren Ihres Nachrichtenflusses einrichten können. Zu Demonstrationszwecken verwenden viele dieser Beispiele die S3-Aktion als Ergebnis.

Anwendungsfall 1: Löschen von Spam für alle Domänen

In diesem Beispiel wird eine globale Regel dargestellt, die Spam-Nachrichten in allen Ihren Domänen löscht. Die Regeln 2 und 3 sollen demonstrieren, das Sie domänenspezifische Regeln anwenden können, nachdem die Spam-Nachrichten in allen Domänen gelöscht wurden.

Regel 1

Empfängerliste: leer Diese Regel gilt daher für alle Empfänger im Rahmen Ihrer verifizierten Domänen.

Aktionen

1. Lambda-Aktion (synchron), die `STOP_RULE_SET` zurückgibt, wenn es sich bei der E-Mail um Spam handelt. Gibt andernfalls `CONTINUE` zurück. Weitere Informationen finden Sie im Beispiel der Lambda-Funktion zum Löschen von Spam-Nachrichten in Beispiele für Lambda-Funktionen.

Regel 2

Empfängerliste: example1.com

Aktionen

1. Jede beliebige Aktion

Regel 3

Empfängerliste: example2.com

Aktionen

1. Jede beliebige Aktion

Anwendungsfall 2: Unzustellbarkeit von Spam für alle Domänen

In diesem Beispiel wird eine globale Regel dargestellt, die Spam-Nachrichten in allen Ihren Domänen als unzustellbar einstuft. Die Regeln 2 und 3 sollen demonstrieren, das Sie domänenspezifische Regeln anwenden können, nachdem die Spam-Nachrichten in allen Domänen als unzustellbar eingestuft wurden.

Regel 1

Empfängerliste: leer Diese Regel gilt daher für alle Empfänger im Rahmen Ihrer verifizierten Domänen.

Aktionen

1. Lambda-Aktion (synchron), die `CONTINUE` zurückgibt, wenn es sich bei der E-Mail um Spam handelt. Gibt andernfalls `STOP_RULE` zurück.
2. Bounce-Aktion ("500 5.6.1. Message content rejected").
3. Stop-Aktion

Regel 2

Empfängerliste: example1.com

Aktionen

1. Jede beliebige Aktion

Regel 3

Empfängerliste: example2.com

Aktionen

1. Jede beliebige Aktion

Anwendungsfall 3: Anwenden der spezifischsten Regel

In diesem Beispiel wird dargestellt, Sie mit der Stoß-Aktion verhindern können, dass E-Mails von mehreren Regeln verarbeitet werden. In diesem Beispiel gibt es eine Regel für eine bestimmte Adresse und eine zweite für alle E-Mail-Adressen der Domäne. Mit der Stop-Aktion werden Nachrichten, die der Regel für die spezifische E-Mail-Adresse entsprechen, nicht von der allgemeineren Regel verarbeitet, die für die Domäne gilt.

Regel 1

Empfängerliste: user@example.com

Aktionen

1. Lambda-Aktion (asynchron)
2. Stop-Aktion

Regel 2

Empfängerliste: example.com

Aktionen

1. Jede beliebige Aktion

Anwendungsfall 4: E-Mail-Ereignisse protokollieren in CloudWatch

In diesem Beispiel wird gezeigt, wie Sie ein Prüfprotokoll aller E-Mails in Ihrem System führen, bevor Sie die E-Mails in Amazon SES speichern.

Regel 1

Empfängerliste: example.com

Aktionen

1. Lambda-Aktion (asynchron), die das Ereignisobjekt in ein CloudWatch Protokoll schreibt. Das Beispiel für Lambda-Funktionen in Beispiele für Lambda-Funktionen log to CloudWatch.
2. S3-Aktion

Anwendungsfall 5: Löschen von E-Mails, die den DKIM-Standard nicht erfüllen

Dieses Beispiel zeigt, wie Sie alle eingehenden E-Mails in einem Amazon-S3-Bucket speichern, aber nur E-Mails, die an eine bestimmte E-Mail-Adresse gerichtet sind und den DKIM-erfüllen, an Ihre automatisierte E-Mail-Anwendung senden.

Regel 1

Empfängerliste: example.com

Aktionen

1. S3-Aktion
2. Lambda-Aktion (synchron), die `STOP_RULE_SET` zurückgibt, wenn die Nachricht den DKIM-Standard nicht erfüllt. Gibt andernfalls `CONTINUE` zurück.

Regel 2

Empfängerliste: support@example.com

Aktionen

1. Lambda-Aktion (asynchron), die die automatisierte Anwendung auslöst.

Anwendungsfall 6: Auf E-Mail basierendes Filtern nach Betreffzeile

Dieses Beispiel zeigt, wie Sie alle eingehenden E-Mails einer Domäne mit dem Wort "Rabatt" in der Betreffzeile löschen und dann die für ein automatisiertes System bestimmte E-Mail auf die eine Art und E-Mails, die an alle anderen Empfänger in der Domäne bestimmt sind, auf eine andere Art verarbeiten.

Regel 1

Empfängerliste: example.com

Aktionen

1. Lambda-Aktion (synchron), die `STOP_RULE_SET` zurückgibt, wenn die Betreffzeile das Wort "Rabatt" enthält. Gibt andernfalls `CONTINUE` zurück.

Regel 2

Empfängerliste: support@example.com

Aktionen

1. S3-Aktion mit Bucket 1.
2. Lambda-Aktion (asynchron), die die automatisierte Anwendung auslöst.
3. Stop-Aktion

Regel 3

Empfängerliste: example.com

Aktionen

1. S3-Aktion mit Bucket 2.
2. Lambda-Aktion (asynchron), die E-Mails für die übrige Domäne verarbeitet.

Beispiele für Lambda-Funktionen

Dieses Thema enthält Beispiele für Lambda-Funktionen, die den Nachrichtenfluss kontrollieren.

Beispiel 1: Löschen von Spam

Dieses Beispiel stoppt die Verarbeitung von Nachrichten mit mindestens einem Spam-Indikator.

```
export const handler = async (event, context, callback) => {
    console.log('Spam filter');

    const sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

    // Check if any spam check failed
    if (sesNotification.receipt.spfVerdict.status === 'FAIL'
            || sesNotification.receipt.dkimVerdict.status === 'FAIL'
            || sesNotification.receipt.spamVerdict.status === 'FAIL'
            || sesNotification.receipt.virusVerdict.status === 'FAIL') {

        console.log('Dropping spam');
```

```
        // Stop processing rule set, dropping message
        callback(null, {'disposition':'STOP_RULE_SET'});
    } else {
        callback(null, {'disposition':'CONTINUE'});
    }
};
```

Beispiel 2: Fortsetzen, wenn ein bestimmter Header gefunden wird

In diesem Beispiel wird die Verarbeitung der aktuellen Regel nur dann fortgesetzt, wenn die E-Mail einen bestimmten Header-Wert enthält.

```
export const handler = async (event, context, callback) => {
    console.log('Header matcher');

    const sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

    // Iterate over the headers
    for (let index in sesNotification.mail.headers) {
        const header = sesNotification.mail.headers[index];

        // Examine the header values
        if (header.name === 'X-Header' && header.value === 'X-Value') {
            console.log('Found header with value.');
            callback(null, {'disposition':'CONTINUE'});
            return;
        }
    }

    // Stop processing the rule if the header value wasn't found
    callback(null, {'disposition':'STOP_RULE'});
};
```

Beispiel 3: Abrufen von E-Mail aus Amazon S3

In diesem Beispiel wird die Raw-E-Mail aus Amazon S3 abgerufen und verarbeitet.

> **Note**
>
> - Sie müssen zunächst die E-Mail mit einer S3-Aktion in Amazon S3 schreiben.

- Stellen Sie sicher, dass die Lambda-Funktion über IAM-Berechtigungen zum Abrufen von Objekten aus dem S3-Bucket verfügt. Weitere Informationen finden Sie in diesem AWS re:POST-Artikel.
- Es ist möglich, dass die standardmäßigen Timeouts für die Lambda-Ausführung zu kurz für Ihren Workflow sind. Erwägen Sie, sie zu erhöhen.

```
import { S3Client, GetObjectCommand } from "@aws-sdk/client-s3";
const bucketName = '<Your Bucket Name>';

export const handler = async (event, context, callback) => {
    const client = new S3Client();
    console.log('Process email');

    var sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));
    console.log("MessageId: " + sesNotification.mail.messageId)

    const getObjectCommand = new GetObjectCommand({
        Bucket: bucketName,
        Key: sesNotification.mail.messageId
    });

    try {
        const response = await client.send(getObjectCommand);
        const receivedMail = await response.Body.transformToString();
        console.log(receivedMail);
        callback(null, {'disposition':'CONTINUE'})
    } catch (e) {
        // Perform error handling here
        console.log("Encountered S3 client error: "+ e, e.stack);
        callback(null, {'disposition':'STOP_RULE_SET'})
    }
};
```

Beispiel 4: Unzustellbarkeit von Nachrichten, bei denen die DMARC-Authentifizierung fehlschlägt

In diesem Beispiel wird eine Unzustellbarkeitsnachricht gesendet, wenn die DMARC-Authentifizierung einer eingehenden E-Mail fehlschlägt.

Note

- Legen Sie bei der Verwendung dieses Beispiels den Wert der Umgebungsvariablen `emailDomain` auf Ihre Domäne für den E-Mail-Empfang fest.
- Stellen Sie sicher, dass die Lambda-Funktion über die `ses:SendBounce` Berechtigungen für die SES-Identität verfügt, die die Bounce-Nachrichten sendet.

```
import { SESClient, SendBounceCommand } from "@aws-sdk/client-ses";
const sesClient = new SESClient();
// Assign the emailDomain environment variable to a constant.
const emailDomain = process.env.emailDomain;

export const handler = async (event, context, callback) => {
    console.log('Spam filter starting');

    const sesNotification = event.Records[0].ses;
    const messageId = sesNotification.mail.messageId;
    const receipt = sesNotification.receipt;

    console.log('Processing message:', messageId);

    // If DMARC verdict is FAIL and the sending domain's policy is REJECT
    // (p=reject), bounce the email.
    if (receipt.dmarcVerdict.status === 'FAIL'
        && receipt.dmarcPolicy.status === 'REJECT') {
        // The values that make up the body of the bounce message.
        const sendBounceParams = {
            BounceSender: `mailer-daemon@${emailDomain}`,
            OriginalMessageId: messageId,
            MessageDsn: {
                ReportingMta: `dns; ${emailDomain}`,
                ArrivalDate: new Date(),
                ExtensionFields: [],
            },
            // Include custom text explaining why the email was bounced.
            Explanation: "Unauthenticated email is not accepted due to the sending
 domain's DMARC policy.",
            BouncedRecipientInfoList: receipt.recipients.map((recipient) => ({
                Recipient: recipient,
                // Bounce with 550 5.6.1 Message content rejected
```

```
                BounceType: 'ContentRejected',
            })),
        };

        console.log('Bouncing message with parameters:');
        console.log(JSON.stringify(sendBounceParams, null, 2));

        const sendBounceCommand = new SendBounceCommand(sendBounceParams);

        // Try to send the bounce.
        try {
          const response = await sesClient.send(sendBounceCommand);
          console.log(response);
          console.log(`Bounce for message ${messageId} sent, bounce message ID:
 ${response.MessageId}`);
          // Stop processing additional receipt rules in the rule set.
          callback(null, {disposition: 'STOP_RULE_SET'});
        } catch (e) {
          // If something goes wrong, log the issue.
          console.log(`An error occurred while sending bounce for message:
 ${messageId}`, e);
          // Perform any additional error handling here
          callback(e)
        }

    // If the DMARC verdict is anything else (PASS, QUARANTINE or GRAY), accept
    // the message and process remaining receipt rules in the rule set.
    } else {
        console.log('Accepting message:', messageId);
        callback(null, {disposition: 'CONTINUE'});
    }
};
```

Aktion „An S3-Bucket liefern“

Die Aktion An S3-Bucket zustellen stellt die E-Mail an einen S3-Bucket zu und kann Sie optional über SNS und mehr benachrichtigen. Diese Aktion umfasst die folgenden Optionen.

- S3-Bucket — Der Name des S3-Buckets, in dem empfangene E-Mails gespeichert werden sollen. Sie können auch einen neuen S3-Bucket erstellen, wenn Sie Ihre Aktion einrichten, indem Sie S3-Bucket erstellen wählen. Amazon SES stellt Ihnen die unformatierte, ungeänderte E-Mail bereit, die in der Regel das Format Multipurpose Internet Mail Extensions (MIME) hat. Weitere Informationen zum MIME-Format finden Sie unter RFC 2045.

> **Important**
>
> - Der Amazon S3 S3-Bucket muss in einer Region existieren, in der SES verfügbar the section called “Empfangen von E-Mails” ist. Andernfalls müssen Sie die unten erläuterte IAM-Rollenoption verwenden.
> - Wenn Sie Ihre E-Mails in einem S3-Bucket speichern, beträgt die standardmäßige maximale E-Mail-Größe (einschließlich Kopfzeilen) 40 MB.
> - SES unterstützt keine Empfangsregeln, die in S3-Buckets hochgeladen werden, die mit einer Objektsperre, die mit einer Standardaufbewahrungsdauer konfiguriert ist, aktiviert sind.
> - Wenn Sie die Verschlüsselung auf Ihren S3-Bucket durch Angabe eines eigenen KMS-Schlüssels anwenden, verwenden Sie unbedingt den vollqualifizierten KMS-Schlüssel-ARN und nicht den KMS-Schlüsselalias. Die Verwendung des Alias kann dazu führen, dass Daten mit einem KMS-Schlüssel verschlüsselt werden, der dem Anforderer und nicht dem Bucket-Administrator gehört. Weitere Informationen finden Sie unter Verwenden von Verschlüsselung für kontenübergreifende Vorgänge.

- Objektschlüsselpräfix — Ein optionales Schlüsselnamenpräfix, das innerhalb des S3-Buckets verwendet werden kann. Mit Schlüsselnamenpräfixen können Sie Ihren S3-Bucket in einer Ordnerstruktur organisieren. Wenn Sie beispielsweise E-Mail als Objektschlüsselpräfix verwenden, werden Ihre E-Mails in Ihrem S3-Bucket in einem Ordner mit dem Namen E-Mail angezeigt.
- Nachrichtenverschlüsselung — Die Option, empfangene E-Mail-Nachrichten zu verschlüsseln, bevor sie an Ihren S3-Bucket gesendet werden.
- KMS-Verschlüsselungsschlüssel — (Verfügbar, wenn Nachrichtenverschlüsselung ausgewählt ist.) Der AWS KMS Schlüssel, den SES verwenden sollte, um Ihre E-Mails zu verschlüsseln, bevor sie im S3-Bucket gespeichert werden. Sie können den Standard-KMS-Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden, den Sie in KMS erstellt haben.

> **Note**
>
> Der von Ihnen gewählte KMS-Schlüssel muss sich in derselben AWS Region befinden wie der SES-Endpunkt, den Sie für den E-Mail-Empfang verwenden.

- Um den Standard-KMS-Schlüssel zu verwenden, wählen Sie aws/ses, wenn Sie die Empfangsregel in der SES-Konsole einrichten. Wenn Sie die SES-API verwenden, können Sie den Standard-KMS-Schlüssel angeben, indem Sie einen ARN in der Form von angeben`arn:aws:kms:REGION:AWSACCOUNTID:alias/aws/ses`. Wenn Ihre AWS Konto-ID beispielsweise 123456789012 lautet und Sie den Standard-KMS-Schlüssel in der Region us-east-1 verwenden möchten, wäre der ARN des Standard-KMS-Schlüssels. `arn:aws:kms:us-east-1:123456789012:alias/aws/ses` Wenn Sie den Standard-KMS-Schlüssel verwenden, müssen Sie keine zusätzlichen Schritte ausführen, um SES die Erlaubnis zur Verwendung des Schlüssels zu erteilen.
- Um einen vom Kunden verwalteten Schlüssel zu verwenden, den Sie in KMS erstellt haben, geben Sie den ARN des KMS-Schlüssels an und stellen Sie sicher, dass Sie der Richtlinie Ihres Schlüssels eine Erklärung hinzufügen, die SES die Erlaubnis zur Verwendung des Schlüssels erteilt. Weitere Informationen zum Erteilen von Berechtigungen finden Sie unter Erteilen von Berechtigungen an Amazon SES für den E-Mail-Empfang.

Weitere Informationen zur Verwendung von KMS mit SES finden Sie im AWS Key Management Service Entwicklerhandbuch. Wenn Sie in der Konsole oder API keinen KMS-Schlüssel angeben, verschlüsselt SES Ihre E-Mails nicht.

> **Important**
>
> Ihre E-Mails werden von SES mithilfe des S3-Verschlüsselungsclients verschlüsselt, bevor sie zur Speicherung an S3 gesendet werden. Sie wird nicht mit serverseitiger S3-Verschlüsselung verschlüsselt. Das bedeutet, dass Sie den S3-Verschlüsselungsclient verwenden müssen, um die E-Mail zu entschlüsseln, nachdem Sie sie von S3 abgerufen haben, da der Dienst keinen Zugriff darauf hat, Ihre KMS-Schlüssel zur Entschlüsselung zu verwenden. Dieser Verschlüsselungs-Client ist in AWS SDK für Java und AWS SDK für Ruby verfügbar. Detaillierte Informationen finden Sie im Konsolenbenutzerhandbuch für Amazon Simple Storage Service.

- IAM-Rolle — Eine IAM-Rolle, die von SES für den Zugriff auf die Ressourcen in der Aktion Deliver to S3 verwendet wird (Amazon S3 S3-Bucket, SNS-Thema und KMS-Schlüssel). Falls nicht angegeben, müssen Sie SES explizit die Berechtigungen erteilen, um auf jede Ressource einzeln zugreifen zu können — siehe. Erteilen von Berechtigungen an Amazon SES für den E-Mail-Empfang

Wenn Sie in einen S3-Bucket schreiben möchten, der in einer Region existiert, in der SES-E-Mail-Empfang nicht verfügbar ist, müssen Sie eine IAM-Rolle verwenden, für die die Zugriffsrichtlinie „In S3 schreiben“ als Inline-Richtlinie der Rolle gilt. Sie können die Berechtigungsrichtlinie für diese Aktion direkt von der Konsole aus anwenden:

1. Wählen Sie im Feld IAM-Rolle die Option Neue Rolle erstellen aus und geben Sie einen Namen gefolgt von Rolle erstellen ein. (Die IAM-Vertrauensrichtlinie für diese Rolle wird automatisch im Hintergrund generiert.)
2. Da die IAM-Vertrauensrichtlinie automatisch generiert wurde, müssen Sie der Rolle nur die Berechtigungsrichtlinie der Aktion hinzufügen. Wählen Sie im Feld IAM-Rolle die Option Rolle anzeigen aus, um die IAM-Konsole zu öffnen.
3. Wählen Sie auf der Registerkarte „Berechtigungen“ die Option „Berechtigungen hinzufügen“ und dann „Inline-Richtlinie erstellen“ aus.
4. Wählen Sie auf der Seite „Berechtigungen angeben“ im Richtlinien-Editor die Option JSON aus.
5. Kopieren Sie die Berechtigungsrichtlinie aus dem IAM-Rollenberechtigungen für die S3-Aktion Richtlinien-Editor, fügen Sie sie ein und ersetzen Sie die Daten im roten Text durch Ihre eigenen. (Achten Sie darauf, jeglichen Beispielcode im Editor zu löschen.)
6. Wählen Sie Weiter aus.
7. Überprüfen und erstellen Sie Ihre Berechtigungsrichtlinie für die IAM-Rolle, indem Sie Richtlinie erstellen wählen.
8. Wählen Sie die Registerkarte Ihres Browsers aus, auf der die SES-Seite Regel erstellen — Aktionen hinzufügen geöffnet ist, und fahren Sie mit den verbleibenden Schritten zum Erstellen von Regeln fort.

- SNS-Thema — Der Name oder ARN des Amazon SNS SNS-Themas, das benachrichtigt werden soll, wenn eine E-Mail im S3-Bucket gespeichert wird. Ein Beispiel für einen ARN für ein SNS-Thema ist arn:aws:sns:us-east - 1:123456789012:. MyTopic Sie können auch ein SNS-Thema erstellen, wenn Sie Ihre Aktion einrichten, indem Sie „SNS-Thema erstellen“ wählen. Weitere Informationen zu SNS-Themen finden Sie im Amazon Simple Notification Service Developer Guide.

> **Note**
>
> - Das von Ihnen gewählte SNS-Thema muss sich in derselben AWS Region befinden wie der SES-Endpunkt, den Sie für den E-Mail-Empfang verwenden.

- Verwenden Sie die vom Kunden verwaltete KMS-Schlüsselverschlüsselung nur für SNS-Themen, die Sie mit den SES-Empfangsregeln verknüpfen, da Sie die KMS-Schlüsselrichtlinie bearbeiten müssen, damit SES auf SNS veröffentlichen kann. Dies steht im Gegensatz zu AWS verwalteten KMS-Schlüsselrichtlinien, die von Haus aus nicht bearbeitet werden können.

Veröffentlichen in einem Amazon SNS-Thema.

Die SNS-Aktion veröffentlicht die E-Mail mit einer Amazon-SNS-Benachrichtigung. Die Benachrichtigung enthält die vollständigen E-Mail-Inhalte. Diese Aktion umfasst die folgenden Optionen.

- SNS Topic – Der Name oder ARN des Amazon-SNS-Themas für die Veröffentlichung der E-Mails. Die Amazon-SNS-Benachrichtigungen enthalten eine unformatierte, unveränderte Kopie der E-Mail, die normalerweise im Multipurpose Internet Mail Extensions (MIME)-Format vorliegt. Weitere Informationen zum MIME-Format finden Sie unter RFC 2045.

  Important

  Wenn Sie Ihre E-Mails über Amazon-SNS-Benachrichtigungen erhalten, beträgt die maximale E-Mail-Größe (einschließlich Header) 150 KB. Größere E-Mails sind unzustellbar. Wenn Sie von größeren E-Mails ausgehen, speichern Sie die E-Mails stattdessen in einem Amazon-S3-Bucket.

  Ein Beispiel für einen Amazon SNS SNS-Themen-ARN ist arn:aws:sns:us-east - 1:123456789012:. MyTopic Sie können ein Amazon-SNS-Thema auch beim Einrichten Ihrer Aktion erstellen, indem Sie Create SNS Topic (SNS-Thema erstellen) auswählen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf Ihre Amazon-SNS-Themen im Amazon Simple Notification Service-Entwicklerleitfaden.

  Note

  - Das von Ihnen Amazon SNS SNS-Thema muss sich in derselben AWS Region befinden wie der Amazon SES SES-Endpunkt, den Sie für den E-Mail-Empfang verwenden.
  - Verwenden Sie die vom Kunden verwaltete KMS-Schlüsselverschlüsselung nur für SNS-Themen, die Sie mit den SES-Empfangsregeln verknüpfen, da Sie die KMS-

Schlüsselrichtlinie bearbeiten müssen, damit SES auf SNS veröffentlichen kann. Dies steht im Gegensatz zu AWS verwalteten KMS-Schlüsselrichtlinien, die von Haus aus nicht bearbeitet werden können.

- Encoding – Die Kodierung, die für die E-Mail in der Amazon-SNS-Benachrichtigung verwendet werden soll. UTF-8 ist einfacher zu verwenden, behält jedoch möglicherweise nicht alle Sonderzeichen bei, wenn eine Nachricht mit einem anderen Codierungsformat kodiert wurde. Base64 bewahrt alle Sonderzeichen. Weitere Informationen zu UTF-8 und Base64 finden Sie in RFC 3629 bzw. RFC 4648.

Wenn Sie E-Mail empfangen, führt Amazon SES die Regeln im aktiven Empfangsregelsatz aus. Sie können mithilfe von Amazon SNS Empfangsregeln konfigurieren, damit Sie Benachrichtigungen erhalten. Ihre Empfangsregeln können zwei verschiedene Arten von Benachrichtigungen senden:

- Von SNS-Aktionen gesendete Benachrichtigungen – Wenn Sie eine SNS;-Aktion zu einer Empfangsregel hinzufügen, werden Informationen über die E-Mail gesendet. Wenn die Nachricht 150 KB oder kleiner ist, enthält dieser Benachrichtigungstyp auch den vollständigen MIME-Text der E-Mail.
- Von anderen Aktionstypen gesendete Benachrichtigungen — Wenn Sie einer Empfangsregel einen anderen Aktionstyp (einschließlich Bounce, Lambda, Stop Rule Set oder WorkMailAktionen) hinzufügen, können Sie optional ein Amazon SNS SNS-Thema angeben. In diesem Fall erhalten Sie Benachrichtigungen, wenn diese Aktionen ausgeführt werden. Diese Benachrichtigung enthalten Informationen über die E-Mail, aber nicht den Inhalt der E-Mail.

In diesem Abschnitt werden die Inhalte der Benachrichtigungen beschrieben und es wird ein Beispiel für jeden Benachrichtigungstyp angegeben:

- Inhalte der Benachrichtigungen für den Amazon-SES-E-Mail-Empfang
- Beispiele für Benachrichtigungen für den Amazon-SES-E-Mail-Empfang

Inhalte der Benachrichtigungen für den Amazon-SES-E-Mail-Empfang

Alle Benachrichtigungen für den E-Mail-Empfang werden unter Amazon Simple Notification Service (Amazon SNS) -Themen im Format JavaScript Object Notation (JSON) veröffentlicht.

Beispielbenachrichtigungen finden Sie unter Benachrichtigungsbeispiele.

Inhalt

- JSON-Objekt der obersten Ebene
- Empfangsobjekt
  - Aktionsobjekt
  - dkimVerdict Object
  - dmarcVerdict Object
  - spamVerdict Object
  - spfVerdict Object
  - virusVerdict Object
- Mail-Objekt
  - commonHeaders-Objekt

JSON-Objekt der obersten Ebene

Das JSON-Objekt der obersten Ebene enthält die folgenden Felder.

Feldname	Description
`notificationType`	Der Benachrichtigungstyp. Für diese Art der Benachrichtigung lautet der Wert immer `Received`.
`receipt`	Ein Objekt, das Informationen über die E-Mail-Zustellung enthält.
`mail`	Ein Objekt, das Informationen zur E-Mail enthält, die der Benachrichtigung zugeordnet ist.
`content`	Eine Zeichenfolge mit der unformatierte, ungeänderten E-Mail, die in der Regel das Format Multipurpose Internet Mail Extensions (MIME) hat. Weitere Informationen zum MIME-Format finden Sie unter RFC 2045.

Feldname	Description
	Note Dieses Feld ist nur dann vorhanden , wenn die Benachrichtigung von einer SNS-Aktion ausgelöst wurde. Benachrichtigungen, die von allen anderen Aktionen ausgelöst werden, die dieses Feld nicht enthalten.

Empfangsobjekt

Das `receipt`-Objekt enthält folgende Felder.

Feldname	Description
`action`	Ein Objekt, das Informationen über die Aktion kapselt, die ausgeführt wurde. Eine Liste möglicher Werte finden Sie unter Aktionsobjekt.
`dkimVerdict`	Objekt, das angibt, ob die DomainKeys Identifie d Mail (DKIM) -Prüfung erfolgreich war. Eine Liste möglicher Werte finden Sie unter dkimVerdict Object.
`dmarcPolicy`	Gibt die DMARC-Einstellungen (Domain-b ased Message Authentication, Reporting & Conformance) für die sendende Domäne an. Dieses Feld wird nur angezeigt, wenn die DMARC-Authentifizierung der Nachricht fehlschlägt. Mögliche Werte für dieses Feld sind: • `none`: Der Eigentümer der sendenden Domäne verlangt, dass bei Nachricht

Feldname	Description
	en, bei denen die DMARC-Authentifizierung fehlschlägt, keine bestimmte Aktion ausgeführt wird. • `quarantine` : Der Eigentümer der sendenden Domäne verlangt, dass Nachrichten, für die die DMARC-Authentifizierung fehlschlägt, von Receivern als verdächtig eingestuft werden. • `reject`: Der Eigentümer der sendenden Domäne verlangt, dass Nachrichten, für die die DMARC-Authentifizierung fehlschlägt, abgelehnt werden.
`dmarcVerdict`	Ein Objekt, das angibt, ob die DMARC-Prüfung (Domain-based Message Authentication, Reporting & Conformance) bestanden wurde. Eine Liste möglicher Werte finden Sie unter dmarcVerdict Object.
`processingTimeMillis`	Eine Zeichenfolge, die den Zeitraum zwischen dem Zeitpunkt, an dem Amazon SES die Nachricht erhalten hat, bis zu dem Zeitpunkt , an dem die Aktion ausgelöst wurde, (in Millisekunden) angibt.
`recipients`	Die Empfänger (speziell die Envelope-RCPT TO-Adressen), die der aktiven Empfangsregel entsprachen. Die hier aufgelisteten Adressen können sich von den Adressen unterscheiden, die von dem Feld `destination` im the section called “Mail-Objekt” aufgelistet werden.

Feldname	Description
spamVerdict	Ein Objekt, das angibt, ob es sich bei der Nachricht um Spam handelt. Eine Liste möglicher Werte finden Sie unter spamVerdict Object.
spfVerdict	Ein Objekt das angibt, ob die Sender Policy Framework (SPF)-Prüfung bestanden wurde. Eine Liste möglicher Werte finden Sie unter spfVerdict Object.
timestamp	Eine Zeichenfolge für Datum und Uhrzeit angibt, zu der die Aktion ausgelöst wurde (im ISO 8601-Format).
virusVerdict	Ein Objekt, das angibt, ob die Nachricht einen Virus enthält. Eine Liste möglicher Werte finden Sie unter virusVerdict Object.

Aktionsobjekt

Das `action`-Objekt enthält folgende Felder.

Feldname	Description
type	Eine Zeichenfolge, die den Typ der Aktion angibt, die ausgeführt wurde. Mögliche Werte sind `S3`, `SNS`, `Bounce`, `Lambda`, `Stop` und `WorkMail`.
topicArn	Eine Zeichenfolge mit dem Amazon-Re ssourcennamen (ARN) des Amazon-SNS-Themas, in der die Benachrichtigung veröffent licht wurde.
bucketName	Eine Zeichenfolge mit dem Namen des Amazon-S3-Buckets, in dem die Benachric

Feldname	Description
	htigung veröffentlicht wurde. Diese ist nur für den S3-Aktionstyp vorhanden.
`objectKey`	Eine Zeichenfolge mit einem eindeutigen Namen für die E-Mail im Amazon-S3-Bucket. Diese Zeichenfolge entspricht der `messageId` im the section called “Mail-Objekt”. Diese ist nur für den S3-Aktionstyp vorhanden.
`smtpReplyCode`	Eine Zeichenfolge mit dem SMTP-Antwortcode gemäß RFC 5321. Diese ist nur für den Bounce-Aktionstyp vorhanden.
`statusCode`	Eine Zeichenfolge mit dem erweiterten SMTP-Statuscode gemäß RFC 3463. Diese ist nur für den Bounce-Aktionstyp vorhanden.
`message`	Eine Zeichenfolge mit dem lesbaren Text für die Unzustellbarkeitsnachricht. Diese ist nur für den Bounce-Aktionstyp vorhanden.
`sender`	Eine Zeichenfolge mit der E-Mail-Adresse des Senders der unzustellbaren E-Mail. Dies ist die Adresse, von der die Unzustellbarkeitsnachricht gesendet wurde. Diese ist nur für den Bounce-Aktionstyp vorhanden.
`functionArn`	Eine Zeichenfolge mit dem ARN der Lambda-Funktion, die ausgelöst wurde. Diese ist nur für den Lambda-Aktionstyp vorhanden.
`invocationType`	Eine Zeichenfolge mit dem Aufruftyp der Lambda-Funktion. Mögliche Werte sind `RequestResponse` und `Event`. Diese ist nur für den Lambda-Aktionstyp vorhanden.

Feldname	Description
`organizationArn`	Zeichenfolge, die den ARN der WorkMail Amazon-Organisation enthält. Nur für den WorkMail Aktionstyp vorhanden.

dkimVerdict Object

Das `dkimVerdict`-Objekt enthält folgende Felder.

Feldname	Description
`status`	Eine Zeichenfolge mit dem DKIM-Prüf ungsergebnis. Die möglichen Werte sind: • `PASS`: Die Nachricht hat die DKIM-Auth entifizierung bestanden. • `FAIL`: Die Nachricht hat die DKIM-Auth entifizierung nicht bestanden. • `GRAY`: Die Nachricht ist nicht DKIM-signiert oder die From-Domäne und die DKIM-Sign aturdomäne stimmen nicht überein. • `PROCESSING_FAILED` : Es ist ein Problem aufgetreten, das verhindert, dass Amazon SES die DKIM-Signatur prüft. DNS-Abfragen schlagen beispielsweise fehl oder der DKIM-Signatur-Header ist nicht ordnungsgemäß formatiert.

dmarcVerdict Object

Das `dmarcVerdict`-Objekt enthält folgende Felder.

Feldname	Description
`status`	Eine Zeichenfolge mit dem DMARC-Prüfungsergebnis. Die möglichen Werte sind: • `PASS`: Die Nachricht hat die DMARC-Authentifizierung bestanden. • `FAIL`: Die DMARC-Authentifizierung für die Nachricht ist fehlgeschlagen. • `GRAY`: Mindestens eine von SPF oder DKIM hat die Authentifizierung bestanden, aber die sendende Domäne hat keine DMARC-Richtlinie oder verwendet die `p=none`-Richtlinie. • `PROCESSING_FAILED` : Es ist ein Problem aufgetreten, das verhindert, dass Amazon SES ein DMARC-Prüfungsergebnis bereitstellt.

spamVerdict Object

Das `spamVerdict`-Objekt enthält folgende Felder.

Feldname	Description
`status`	Eine Zeichenfolge mit dem Ergebnis der Prüfung auf Spam. Die möglichen Werte sind: • `PASS`: Die Prüfung auf Spam hat ergeben, dass die Nachricht wahrscheinlich keinen Spam enthält. • `FAIL`: Die Prüfung auf Spam hat ergeben, dass die Nachricht wahrscheinlich Spam enthält. • `GRAY`: Amazon SES; hat die E-Mail geprüft, konnte aber nicht mit Sicherheit ermitteln, ob es sich um Spam handelt.

Feldname	Description
	• `PROCESSING_FAILED` : Amazon SES konnte die E-Mail nicht prüfen. Bei der E-Mail handelt es sich beispielsweise nicht um eine gültige MIME-Nachricht.

spfVerdict Object

Das `spfVerdict`-Objekt enthält folgende Felder.

Feldname	Description
`status`	Eine Zeichenfolge mit dem SPF-Prüfungsergebnis. Die möglichen Werte sind: • `PASS`: Die Nachricht hat die SPF-Authentifizierung bestanden. • `FAIL`: Die Nachricht hat die SPF-Authentifizierung nicht bestanden. • `GRAY`: Das SPF-Ergebnis lautet `none`, `softfail` oder `neutral`. • `PROCESSING_FAILED` : Es ist ein Problem aufgetreten, das verhindert, dass Amazon SES den SPF-Datensatz prüft. DNS-Abfragen schlagen beispielsweise fehl.

virusVerdict Object

Das `virusVerdict`-Objekt enthält folgende Felder.

Feldname	Description
`status`	Eine Zeichenfolge mit dem Ergebnis der Virusprüfung. Die möglichen Werte sind: • `PASS`: Die Nachricht enthält keine Viren.

Feldname	Description
	• `FAIL`: Die Nachricht enthält einen Virus. • `GRAY`: Amazon SES hat die E-Mail geprüft, konnte aber nicht mit Sicherheit ermitteln, ob sie einen Virus enthält. • `PROCESSING_FAILED` : Amazon SES kann den Inhalt der E-Mail nicht prüfen. Bei der E-Mail handelt es sich beispielsweise nicht um eine gültige MIME-Nachricht.

Mail-Objekt

Das `mail`-Objekt enthält folgende Felder.

Feldname	Description
`destination`	Eine vollständige Liste aller Empfänger adressen (einschließlich To: – und CC: - Empfänger) aus den MIME-Headern der eingehenden E-Mail.
`messageId`	Eine Zeichenfolge mit der eindeutigen ID, die der E-Mail von Amazon SES zugewiesen wurde. Wenn die E-Mail-Nachricht Amazon S3 zugestellt wurde, ist die Mitteilungs-ID gleichzei tig der Amazon-S3-Objektschlüssel, mit dem die Nachricht in Ihren Amazon-S3-Bucket geschrieben wurde.
`source`	Eine Zeichenfolge mit der E-Mail-Adresse (speziell der Envelope-MAIL FROM-Adresse), von der die E-Mail gesendet wurde.
`timestamp`	Zeichenfolge, die die Uhrzeit des Empfangs der E-Mail im ISO8601 Format enthält.

Feldname	Description
`headers`	Die Amazon-SES-Header und Ihre benutzerd efinierten Header. Jeder Header enthält die folgenden Felder: `name` und `value`.
`commonHeaders`	Die für alle E-Mails gemeinsamen Header. Jeder Header enthält die folgenden Felder: `name` und `value`.
`headersTruncated`	Eine Zeichenfolge, die angibt, ob die Header in der Benachrichtigung abgeschnitten wurden. Dies passiert, wenn die Header größer als 10 KB sind. Mögliche Werte sind `true` und `false`.

commonHeaders-Objekt

Das `commonHeaders`-Objekt kann die in der folgenden Tabelle angegebenen Felder enthalten. Die Felder in diesem Objekt variieren je nachdem, welche Felder in der eingehenden E-Mails vorhanden waren.

Feldname	Description
`messageId`	Die ID der ursprünglichen Nachricht.
`date`	Datum und Uhrzeit, als Amazon SES die Nachricht erhalten hat.
`to`	Die To (EN)-Header der E-Mail.
`cc`	Die CC (EN)-Header der E-Mail.
`bcc`	Die BCC (EN)-Header der E-Mail.
`from`	Die From (EN)-Header der E-Mail.
`sender`	Die Sender (EN)-Header der E-Mail.

Feldname	Description
`returnPath`	Die Return-Path (EN)-Header der E-Mail.
`replyTo`	Die Reply-To (EN)-Header der E-Mail.
`subject`	Die Subject (EN)-Header der E-Mail.

Beispiele für Benachrichtigungen für den Amazon-SES-E-Mail-Empfang

Dieser Abschnitt enthält Beispiele für die folgenden Arten von Benachrichtigungen:

- Eine Benachrichtigung, die als Ergebnis einer SNS-Aktion gesendet wurde.
- Eine Benachrichtigung, die aufgrund einer anderen Art der Aktion gesendet wird (eine Warnungsbenachrichtigung).

Benachrichtigung über eine SNS-Aktion

Dieser Abschnitt enthält ein Beispiel für eine Benachrichtigung über eine SNS-Aktion. Im Gegensatz zu der vorher genannten Warnungsbenachrichtigung enthält sie einen `content`-Abschnitt mit der E-Mail, die in der Regel im Format Multipurpose Internet Mail Extensions (MIME) vorliegt.

```
{
  "notificationType":"Received",
  "receipt":{
    "timestamp":"2015-09-11T20:32:33.936Z",
    "processingTimeMillis":222,
    "recipients":[
      "recipient@example.com"
    ],
    "spamVerdict":{
      "status":"PASS"
    },
    "virusVerdict":{
      "status":"PASS"
    },
    "spfVerdict":{
      "status":"PASS"
    },
    "dkimVerdict":{
```

```
      "status":"PASS"
    },
    "action":{
      "type":"SNS",
      "topicArn":"arn:aws:sns:us-east-1:012345678912:example-topic"
    }
  },
  "mail":{
    "timestamp":"2015-09-11T20:32:33.936Z",
    "source":"61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com",
    "messageId":"d6iitobk75ur44p8kdnnp7g2n800",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"Return-Path",

"value":"<0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com>"
      },
      {
        "name":"Received",
        "value":"from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
[54.240.9.183]) by inbound-smtp.us-east-1.amazonaws.com with SMTP id
d6iitobk75ur44p8kdnnp7g2n800 for recipient@example.com; Fri, 11 Sep 2015 20:32:33
+0000 (UTC)"
      },
      {
        "name":"DKIM-Signature",
        "value":"v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
s=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;
h=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID; bh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;
b=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF
hlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g="
      },
      {
        "name":"From",
        "value":"sender@example.com"
      },
      {
        "name":"To",
```

```
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Example subject"
      },
      {
        "name":"MIME-Version",
        "value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"text/plain; charset=UTF-8"
      },
      {
        "name":"Content-Transfer-Encoding",
        "value":"7bit"
      },
      {
        "name":"Date",
        "value":"Fri, 11 Sep 2015 20:32:32 +0000"
      },
      {
        "name":"Message-ID",
        "value":"<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>"
      },
      {
        "name":"X-SES-Outgoing",
        "value":"2015.09.11-54.240.9.183"
      },
      {
        "name":"Feedback-ID",
        "value":"1.us-east-1.Krv2FKpFdWV+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES"
      }
    ],
    "commonHeaders":{

  "returnPath":"0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
      "from":[
        "sender@example.com"
      ],
      "date":"Fri, 11 Sep 2015 20:32:32 +0000",
      "to":[
        "recipient@example.com"
```

```
      ],
      "messageId":"<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>",
      "subject":"Example subject"
    }
  },
  "content":"Return-Path: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>\r
\nReceived: from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
 [54.240.9.183])\r\n by inbound-smtp.us-east-1.amazonaws.com with SMTP id
 d6iitobk75ur44p8kdnnp7g2n800\r\n for recipient@example.com;\r\n Fri, 11 Sep 2015
 20:32:33 +0000 (UTC)\r\nDKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/
simple;\r\n\ts=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;\r\n
\th=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID;\r\n\tbh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;\r\n
\tb=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF\r\n
\thlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX\r\n
\t4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g=\r\nFrom: sender@example.com\r\nTo:
 recipient@example.com\r\nSubject: Example subject\r\nMIME-Version: 1.0\r\nContent-
Type: text/plain; charset=UTF-8\r\nContent-Transfer-Encoding: 7bit\r\nDate: Fri, 11 Sep
 2015 20:32:32 +0000\r\nMessage-ID: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>
\r\nX-SES-Outgoing: 2015.09.11-54.240.9.183\r\nFeedback-ID: 1.us-east-1.Krv2FKpFdWV
+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES\r\n\r\nExample content\r\n"
}
```

Warnungsbenachrichtigung

Dieser Abschnitt enthält ein Beispiel für eine Amazon-SNS-Benachrichtigung, die von einer S3-Aktion ausgelöst werden kann. Benachrichtigungen, die von Lambda-, Bounce-, Stop- und WorkMail -Aktionen ausgelöst werden, sind ähnlich. Obwohl die Benachrichtigung Informationen über die E-Mail enthält, ist der Inhalt der eigentlichen E-Mail nicht angegeben.

```
{
     "notificationType": "Received",
    "receipt": {
      "timestamp": "2015-09-11T20:32:33.936Z",
      "processingTimeMillis": 406,
      "recipients": [
        "recipient@example.com"
      ],
      "spamVerdict": {
        "status": "PASS"
      },
      "virusVerdict": {
        "status": "PASS"
```

```
      },
      "spfVerdict": {
        "status": "PASS"
      },
      "dkimVerdict": {
        "status": "PASS"
      },
      "action": {
        "type": "S3",
        "topicArn": "arn:aws:sns:us-east-1:012345678912:example-topic",
        "bucketName": "my-S3-bucket",
        "objectKey": "\email"
      }
    },
    "mail": {
      "timestamp": "2015-09-11T20:32:33.936Z",
      "source":
 "0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
      "messageId": "d6iitobk75ur44p8kdnnp7g2n800",
      "destination": [
        "recipient@example.com"
      ],
      "headersTruncated": false,
      "headers": [
        {
          "name": "Return-Path",
          "value":
 "<0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com>"
        },
        {
          "name": "Received",
          "value": "from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
 [54.240.9.183]) by inbound-smtp.us-east-1.amazonaws.com with SMTP id
 d6iitobk75ur44p8kdnnp7g2n800 for recipient@example.com; Fri, 11 Sep 2015 20:32:33
 +0000 (UTC)"
        },
        {
          "name": "DKIM-Signature",
          "value": "v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
 s=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;
 h=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID; bh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;
 b=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF
```

```
hlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g="
       },
       {
         "name": "From",
         "value": "sender@example.com"
       },
       {
         "name": "To",
         "value": "recipient@example.com"
       },
       {
         "name": "Subject",
         "value": "Example subject"
       },
       {
         "name": "MIME-Version",
         "value": "1.0"
       },
       {
         "name": "Content-Type",
         "value": "text/plain; charset=UTF-8"
       },
       {
         "name": "Content-Transfer-Encoding",
         "value": "7bit"
       },
       {
         "name": "Date",
         "value": "Fri, 11 Sep 2015 20:32:32 +0000"
       },
       {
         "name": "Message-ID",
         "value": "<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>"
       },
       {
         "name": "X-SES-Outgoing",
         "value": "2015.09.11-54.240.9.183"
       },
       {
         "name": "Feedback-ID",
         "value": "1.us-east-1.Krv2FKpFdWV+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES"
       }
     ],
```

```
      "commonHeaders": {
        "returnPath":
"0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
        "from": [
          "sender@example.com"
        ],
        "date": "Fri, 11 Sep 2015 20:32:32 +0000",
        "to": [
          "recipient@example.com"
        ],
        "messageId": "<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>",
        "subject": "Example subject"
      }
    }
  }
```

Aktion „Regelsatz beenden“

Die Stop-Aktion beendet die Auswertung des Empfangsregelsatzes und benachrichtigt Sie optional über Amazon SNS. Diese Aktion umfasst die folgenden Optionen.

- SNS Topic– Der Name oder ARN des Amazon-SNS-Themas, das benachrichtigt werden soll, wenn die angegebene Stop-Aktion ausgeführt wird. Ein Beispiel für einen Amazon SNS SNS-Themen-ARN ist arn:aws:sns:us-east - 1:123456789012:. MyTopic Sie können ein Amazon-SNS-Thema auch beim Einrichten Ihrer Aktion erstellen, indem Sie Create SNS Topic (SNS-Thema erstellen) auswählen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf Ihre Amazon-SNS-Themen im Amazon Simple Notification Service-Entwicklerleitfaden.

  > **Note**
  >
  > Das von Ihnen Amazon SNS SNS-Thema muss sich in derselben AWS Region befinden wie der Amazon SES SES-Endpunkt, den Sie für den E-Mail-Empfang verwenden.

Mit Amazon WorkMail Action integrieren

Die WorkMailAktion ist in Amazon integriert WorkMail. Wenn Amazon Ihre gesamte E-Mail-Verarbeitung WorkMail durchführt, verwenden Sie diese Aktion normalerweise nicht direkt, da Amazon sich um die Einrichtung WorkMail kümmert. Diese Aktion umfasst die folgenden Optionen.

- Organisations-ARN — Der ARN der WorkMail Amazon-Organisation. WorkMail Amazon-Organisationen ARNs haben die Formarn:aws:workmail:*region*:*account_ID*:organization/*organization_ID*, in der:
  - `region`ist die Region, in der Sie Amazon SES und Amazon verwenden WorkMail. (Sie müssen sie in der gleichen Region verwenden.) Ein Beispiel ist us-east-1.
  - `account_ID`ist die AWS Konto-ID. Sie finden Ihre AWS Konto-ID auf der Kontoseite der AWS Management Console.
  - `organization_ID`ist eine eindeutige Kennung, die Amazon WorkMail generiert, wenn Sie eine Organisation erstellen. Sie finden die Organisations-ID in der WorkMail Amazon-Konsole auf der Seite mit den Organisationseinstellungen Ihrer Organisation.

  Ein Beispiel für einen vollständigen WorkMail Amazon-Organisations-ARN ist arn:aws:workmail:us-east- 1:123456789012:organization/m-68755160c4cb4e29a2b2f8fb58f359d7. Informationen zu WorkMail Amazon-Organisationen finden Sie im WorkMail Amazon-Administratorhandbuch.
- SNS-Thema— Der Name oder ARN des Amazon SNS SNS-Themas, das benachrichtigt werden soll, wenn die WorkMail Amazon-Aktion ergriffen wird. Ein Beispiel für einen Amazon SNS SNS-Themen-ARN ist arn:aws:sns:us-east - 1:123456789012:. MyTopic Sie können ein Amazon-SNS-Thema auch beim Einrichten Ihrer Aktion erstellen, indem Sie Create SNS Topic (SNS-Thema erstellen) auswählen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf Ihre Amazon-SNS-Themen im Amazon Simple Notification Service-Entwicklerleitfaden.

  > **Note**
  >
  > Das von Ihnen Amazon SNS SNS-Thema muss sich in derselben AWS Region befinden wie der Amazon SES SES-Endpunkt, den Sie für den E-Mail-Empfang verwenden.

> **Note**
>
> Amazon SES unterstützt nur WorkMail Aktionen in Regionen, in denen WorkMail es verfügbar ist. Informationen zu WorkMail Amazon-Endpunkten und -Kontingenten finden Sie in der Allgemeine AWS-Referenz.

Exemplarische Vorgehensweise bei der Konfiguration von IP-Adressenfiltern

In diesem Abschnitt erfahren Sie, wie Sie IP-Adressfilter über die Amazon SES Konsole einrichten. Mit der IP-Adressfilterung können Sie ein breites Maß an Kontrolle bereitstellen. Mit diesen IP-Filtern können Sie alle Nachrichten aus bestimmten IP-Adressen oder IP-Adressbereichen explizit blockieren oder zulassen.

Optional können Sie das`CreateReceiptFilter`-API verwenden, um einen IP-Adressenfilter zu erstellen, wie imAmazon Simple Email Service API-Referenzaus.

> **Note**
>
> Wenn Sie nur E-Mails von einer endlichen Liste bekannter IP-Adressen erhalten möchten, richten Sie eine Blockierungsliste mit `0.0.0.0/0` und eine Freigabeliste ein, die die IP-Adressen enthält, denen Sie vertrauten. Diese Konfiguration blockiert alle IP-Adressen standardmäßig und lässt nur E-Mails von den IP-Adressen zu, die Sie explizit angeben.

Voraussetzungen

Die folgenden Voraussetzungen müssen erfüllt sein, bevor Sie mit der Einrichtung der empfängerbasierten E-Mail-Steuerung mithilfe von IP-Adressfiltern fortfahren:

1. Sie müssen zuerstErstellen und Überprüfen einer Domänen-IdentitätAmazon SES.
2. Als Nächstes müssen Sie angeben, welche Mail-Server E-Mails für Ihre Domain akzeptieren können, indem SieVeröffentlichen eines MX-Datensatzesauf die DNS-Einstellungen Ihrer Domäne. (Der MX-Eintrag sollte sich auf den Amazon SES-Endpunkt beziehen, der E-Mails für die AWS Region empfängt, in der Sie Amazon SES verwenden.)

Erstellen von IP-Adressenfilter

So erstellen Sie einen IP-Adressenfilter (Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Email Receiving aus.

3. Wählen Sie die Registerkarte IP address filters (IP-Adressenfilter).
4. Wählen Sie Create Filter (Filter erstellen).
5. Geben Sie einen eindeutigen Namen für Ihren Filter ein. Die Legende des Felds zeigt die Syntaxanforderungen an. Der Name muss weniger als 64 alphanumerische Zeichen, Bindestriche (-), Unterstriche (_), Punkte (.) enthalten.
6. Geben Sie eine IP-Adresse oder einen Bereich von IP-Adressen ein. Die Legende des Feldes enthält Beispiele, die in der Classless Inter-Domain Routing (CIDR) -Syntax angegeben sind. (Ein Beispiel für eine einzelne IP-Adresse ist 10.0.0.1. Ein IP-Adressenbereich ist beispielsweise 10.0.0.1/24. Weitere Informationen zur CIDR-Notation finden Sie unterRFC 2317.)
7. Wählen Sie Policy type (Richtlinientyp), indem Sie entweder das Optionsfeld Block (Blockieren) oder Allow (Erlauben) auswählen.
8. Wählen Sie Create Filter) (Filter erstellen.
9. Wenn Sie einen anderen IP-Filter hinzufügen möchten, wählen Sie Create filter (Filter erstellen) und wiederholen Sie die vorherigen Schritte für jeden zusätzlichen Filter, den Sie hinzufügen möchten.
10. Wenn Sie einen IP-Adressfilter entfernen möchten, wählen Sie ihn aus und wählen Sie die Schaltfläche Delete (Löschen).

Anzeigen von Metriken für den Amazon-SES-E-Mail-Empfang

Wenn Sie den E-Mail-Empfang in Amazon SES aktiviert und Empfangsregeln für Ihre E-Mail erstellt haben, können Sie die Metriken für diese Empfangsregelsätze und -regeln über Amazon einsehen CloudWatch.

In der CloudWatch Konsole finden Sie die Metriken unter Metriken > Alle Metriken > SES > Empfangsregelsatz-Metriken und Empfangsregel-Metriken.

> **Note**
>
> Damit Empfangsregelsatzmetriken und Empfangsregelmetriken unter SES angezeigt werden, müssen Sie folgende Schritte ausgeführt haben:
>
> - E-Mail-Empfang aktivieren
> - Empfangsregeln erstellen
> - eine E-Mail erhalten, die einer Ihrer Regeln entspricht.

Die folgenden Nachrichtenmetriken sind verfügbar:

- Nachrichtenempfang

Scope	Metrik	Beschreibung	Dimension
Empfangsregelsatzmetriken	Empfangen	SES hat erfolgreich eine Nachricht erhalten, für die mindestens eine Regel gilt. Diese Metrik darf nur den Wert 1 haben.	RuleSetName
Empfangsregelmetriken	Empfangen	SES hat erfolgreich eine Nachricht erhalten und wird versuchen, die angewendete Regel zu verarbeiten. Diese Metrik darf nur den Wert 1 haben.	RuleName

- Nachrichten veröffentlichen

Scope	Metrik	Beschreibung	Dimension
Empfangsregelsatzmetriken	PublishSuccess	SES hat erfolgreich alle Regeln ausgeführt, die innerhalb eines Regelsatzes gelten.	RuleSetName
Empfangsregelmetriken	PublishSuccess	SES hat erfolgreich eine Regel ausgeführt, die für die Empfangsnachricht gilt.	RuleName
Empfangsregelsatzmetriken	PublishFailure	SES ist beim Versuch, Regeln innerhalb eines Regelsatzes auszuführen, auf einen Fehler gestoßen. Die Ausführung wird erneut versucht.	RuleSetName
Empfangsregelmetriken	PublishFailure	Bei SES ist beim Versuch, die Aktionen in einer Regel auszuführen, ein Fehler aufgetreten. Je nach Fehler wird die Ausführung ggf. erneut versucht.	RuleName
Empfangsregelsatzmetriken	PublishExpired	SES versucht nicht mehr, die Regeln auszuführen, weil sie innerhalb von 36 Stunden nicht erfolgreich waren oder weil ein	RuleSetName

Scope	Metrik	Beschreibung	Dimension
		Fehler aufgetreten ist, der nicht wiederher stellbar ist.	
Empfangsr egelmetriken	PublishEx pired	SES wird nicht mehr erneut versuchen, die Aktionen der Regel auszuführen, da sie innerhalb von 36 Stunden nicht erfolgreich waren.	RuleName

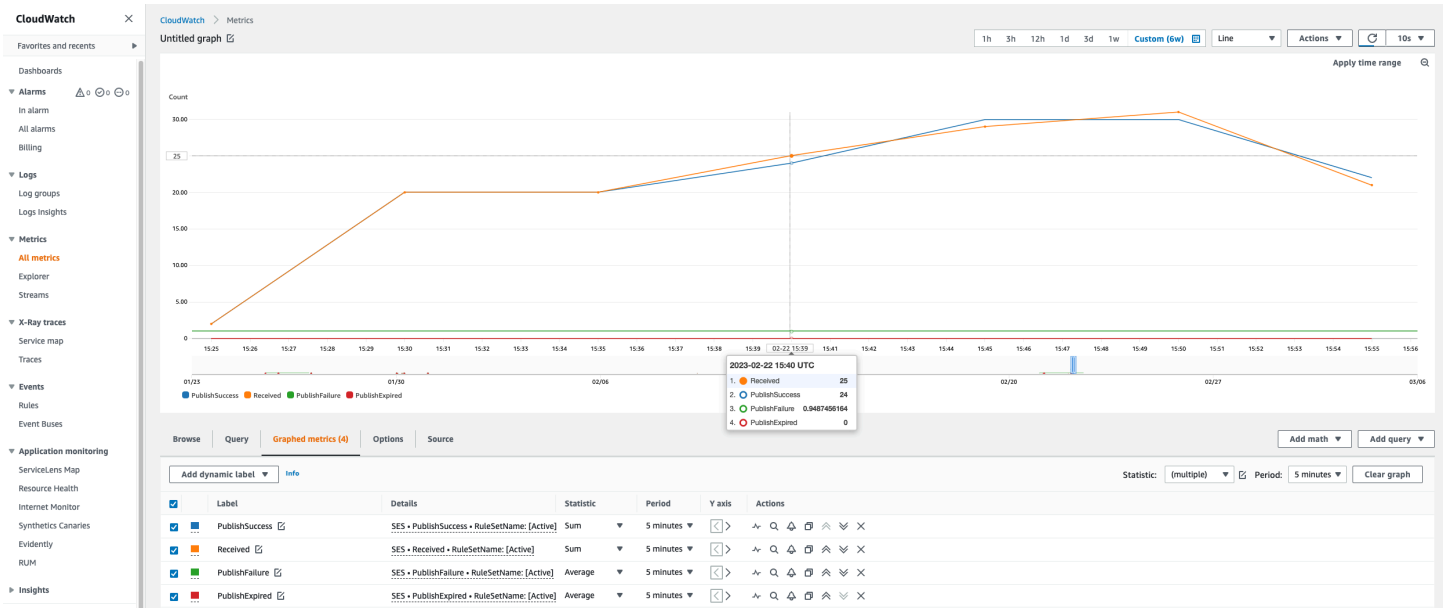
Note

- In den vorherigen Tabellen bedeutet der Begriff gelten bzw. anwenden, dass der Absender nicht von IP-Filtern gesperrt wird oder auf der internen Blockierliste von SES steht und dass die Regel über übereinstimmende Empfängerbedingungen und eine entsprechende TLS-Richtlinie verfügt.
- PublishFailure-Fehler können z. B. auftreten, wenn Sie die Berechtigungen für einen Amazon-S3-Bucket, ein Amazon-SNS-Thema oder eine Lambda-Funktion gelöscht oder widerrufen haben, für die eine Aktion in einer Ihrer Empfangsregeln konfiguriert war.
- Da jeweils nur ein Regelsatz aktiv sein kann, veröffentlicht SES eine aggregierte Metrik, die wie folgt angezeigt wird RuleSetName: [Aktiv] für alle Regelsätze, die für den von Ihnen ausgewählten Zeitraum aktiv waren. CloudWatch Dies hat den Vorteil, dass Sie Regelsätze frei ändern können, ohne Ihre Alarmkonfiguration anzupassen.

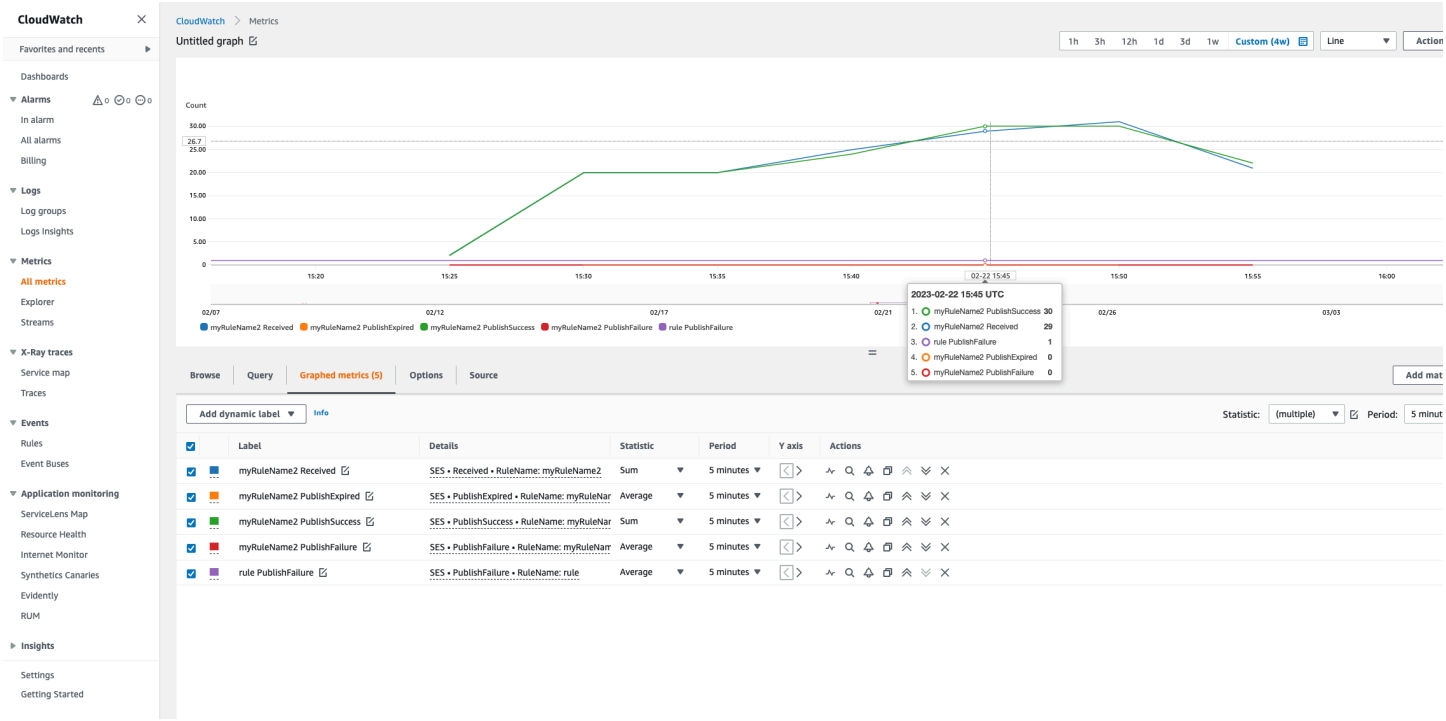
Important

Änderungen, die Sie an Ihrem Empfangsregelsatz vornehmen, werden nur für E-Mails angewendet, die Amazon SES nach der Aktualisierung empfängt. E-Mails werden stets in Bezug auf den Empfangsregelsatz ausgewertet, der zum Zeitpunkt des E-Mail-Empfangs aktiv war.

Metriken für einen SES-Empfangsregelsatz, die in der CloudWatch Konsole angezeigt werden.



Metriken für eine SES-Empfangsregel, die in der CloudWatch Konsole angezeigt werden.



Mandanten

In diesem Kapitel wird erklärt, wie Sie Amazon SES Tenant Management verwenden, um den E-Mail-Versand zwischen mehreren Mandanten innerhalb Ihres SES-Kontos zu isolieren, zu überwachen und zu verwalten. Diese Funktion unterstützt unabhängige Softwareanbieter (ISVs), Unternehmen und Organisationen, die E-Mails im Namen mehrerer nachgelagerter Einheiten versenden, dabei, separate Reputationsprofile zu verwalten und zu verhindern, dass Probleme mit einem Mandanten andere beeinflussen.

Was ist Mandantenverwaltung?

Die Mandantenverwaltung ist eine Funktion, mit der Sie isolierte Container, sogenannte „Mandanten“, in Ihrem SES-Konto erstellen können. Jeder Mandant kann seine eigenen E-Mail-Identitäten, Konfigurationssätze, Vorlagen und Reputationsmetriken haben, wodurch sichergestellt wird, dass die E-Mail-Aktivitäten vollständig zwischen verschiedenen Kunden oder Geschäftsbereichen getrennt sind.

Das Mandantenmanagement befasst sich mit der Herausforderung, dass die schlechten E-Mail-Praktiken eines Kunden zuvor dazu geführt haben, dass ein ganzes SES-Konto unterbrochen wurde, was sich auf alle anderen Kunden auswirkte. Mit der Mandantenisolierung können Sie mehrere E-Mail-Streams unabhängig voneinander verwalten und gleichzeitig die zentrale Überwachung und Kontrolle beibehalten.

Ein Mandant dient als logischer Container, der verwandte SES-Ressourcen zusammenfasst. Wenn Sie E-Mails im Namen eines bestimmten Mandanten versenden, verfolgt SES die Reputationsmetriken und setzt Richtlinien auf Mandantenebene durch. Diese Isolierung stellt sicher, dass eine hohe Absprungrate oder Beschwerderate von einem Mandanten die Zustellbarkeit von E-Mails anderer Mieter nicht beeinträchtigt.

Das Mietermanagement ist besonders wertvoll für:

- Unabhängige Softwareanbieter (ISVs), die E-Mails im Namen mehrerer Kunden versenden.
- Unternehmen, die E-Mail-Kommunikation zwischen verschiedenen Geschäftsbereichen verwalten.
- Dienstanbieter, die die E-Mail-Reputation nach Kunden oder Anwendungen isolieren müssen.
- Organizations, die die Einhaltung unterschiedlicher regulatorischer Anforderungen pro Mieter benötigen.

Wie funktioniert die Mieterverwaltung

Tenant Reputation Management funktioniert, indem ein logischer Container für Ihre E-Mail-Versandressourcen erstellt wird. Sie weisen jedem Mandanten bestimmte Ressourcen zu, darunter verifizierte Identitäten (Domänen und E-Mail-Adressen), Konfigurationssätze und Vorlagen. Wenn Sie E-Mails im Namen eines Mandanten senden, geben Sie den Mandanten in Ihrem API-Aufruf oder SMTP-Header an, und SES überprüft, ob die verwendeten Ressourcen diesem Mandanten ordnungsgemäß zugeordnet sind.

Zuordnung der Ressourcen

Ressourcen in Ihrem SES-Konto können Mandanten auf zwei Arten zugeordnet werden:

- Dedizierte Zuweisung — Ressourcen, die ausschließlich von bestimmten Mandanten genutzt werden.
- Gemeinsame Zuweisung — Ressourcen, die mehreren Mandanten zur Verfügung stehen.

Wenn Sie eine Ressource einem Mandanten zuordnen, erhält dieser Mandant die Erlaubnis, diese Ressource für den E-Mail-Versand zu verwenden. Bei jeder Sendeanfrage überprüft SES, ob der angegebene Mandant berechtigt ist, die Identität, den Konfigurationssatz und die Vorlage in der Anfrage zu verwenden. Wenn die Ressourcen nicht richtig zugeordnet sind, schlägt die Sendeanforderung fehl.

Reputationsüberwachung und Durchsetzung

SES überwacht kontinuierlich die wichtigsten Reputationskennzahlen für jeden Mandanten, darunter Absprungraten, Beschwerdequoten (einschließlich der vom Feedback Loop (FBL) -System des Postfachanbieters ausgegebenen) und Feedback-Signale von Drittanbietern. Wenn diese Kennzahlen definierte Schwellenwerte überschreiten, erstellt SES „Reputationsergebnisse“, die wie folgt kategorisiert sind:

- Warnungen mit geringem Schweregrad — Kleinere Probleme, die die Zustellbarkeit beeinträchtigen könnten, wenn sie nicht behoben werden.
- Warnungen mit hohem Schweregrad — Schwerwiegende Probleme, die sich wahrscheinlich auf die Zustellbarkeit auswirken und zu deren Durchsetzung führen können.

Auf der Grundlage dieser Ergebnisse kann SES problematische Mandanten mithilfe von von Ihnen konfigurierten Reputationsrichtlinien automatisch pausieren. Drei Durchsetzungsstufen sind verfügbar:

- Standard (empfohlen) — Unterbricht das Senden von Mandanten automatisch, wenn Reputationsbefunde mit hohem Schweregrad erkannt werden. Dies bietet einen ausgewogenen Schutz und minimiert gleichzeitig Unterbrechungen.
- Streng — Unterbricht das Senden von Mandanten automatisch, wenn ein Reputationsproblem erkannt wird, auch bei Problemen mit geringem Schweregrad. Bietet maximalen Schutz, kann jedoch zu häufigeren Unterbrechungen führen.
- Keine — Deaktiviert das automatische Anhalten für den Mandanten. Alle Reputationsergebnisse werden weiterhin aufgezeichnet und sind sichtbar, es werden jedoch keine automatisierten Durchsetzungsmaßnahmen ergriffen.

Wenn die Metriken eines Mandanten eine Reputationsfeststellung auslösen, die den Schwellenwert für die Durchsetzung gemäß Ihrer ausgewählten Richtlinie erreicht, aktualisiert das System den Sendestatus des Mandanten automatisch auf „Unterbrochen“, ohne die Sendefähigkeit anderer Mandanten zu beeinträchtigen. Solange ein Mandant pausiert ist, schlägt jeder Versuch, E-Mails über diesen Mandanten zu versenden, fehl, bis Sie das Problem geprüft und das Senden manuell wieder aktiviert haben. Darüber hinaus können Sie die Sendefunktionen eines Mandanten bei Bedarf manuell unterbrechen und die Pause wieder aufheben, wenn Sie bereit sind, den Versand fortzusetzen.

Mieter einrichten

Themen

- Mieter erstellen
- Einem Mandanten Ressourcen zuweisen
- Konfiguration von Reputationsrichtlinien

Mieter erstellen

Mit der Konsole:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die SES-Konsole unter https://console.aws.amazon.com/ses/.

2. Wählen Sie im Navigationsbereich Tenants aus.
3. Wählen Sie Mandant erstellen aus.
4. Geben Sie unter Mandantenname einen eindeutigen Namen für Ihren Mandanten ein.
5. Wählen Sie „Mandant erstellen“.

Verwenden von AWS CLI:

```
aws sesv2 create-tenant \
    --tenant-name "MyTenant" \
    --region us-east-1
```

Einem Mandanten Ressourcen zuweisen

Nach dem Erstellen eines Mandanten müssen Sie mindestens eine verifizierte Identität und einen Konfigurationssatz zuweisen, bevor der Mandant E-Mails senden kann.

Mithilfe der Konsole:

1. Navigieren Sie in der SES-Konsole zur Seite Mandanten.
2. Wählen Sie den Mandanten aus, den Sie konfigurieren möchten.
3. Im Bereich Mandantenkonfiguration können Sie die Karten Identitäten und Konfigurationssätze verwenden, um diese Ressourcen zuzuweisen. Optional können Sie zum Bereich mit den Registerkarten nach unten scrollen und die Registerkarten Identitäten und Konfigurationssätze verwenden, um dasselbe zu tun.

   > **Note**
   >
   > Jeder Versuch, eine Identität oder einen Konfigurationssatz zu löschen, der einem Mandanten zugeordnet ist, schlägt fehl. Sie müssen diese Verknüpfungen zuerst aus dem Mandanten entfernen, bevor Sie die zugehörigen Ressourcen löschen können.

4. (Optional) Sie können Ihrem Mandanten ein oder mehrere Tags zuweisen, indem Sie die Registerkarte Tags auswählen.

Verwenden von AWS CLI:

```
# Assign an identity to a tenant
```

```
aws sesv2 create-tenant-resource-association \
    --tenant-name "MyTenant" \
    --resource-arn "arn:aws:ses:us-east-1:123456789012:identity/example.com" \
    --region us-east-1

# Assign a configuration set to a tenant
aws sesv2 create-tenant-resource-association \
    --tenant-name "MyTenant" \
    --resource-arn "arn:aws:ses:us-east-1:123456789012:configuration-set/MyConfigSet" \
    --region us-east-1
```

Konfiguration von Reputationsrichtlinien

Reputationsrichtlinien legen anhand von Reputationsmetriken fest, wann der E-Mail-Versand eines Mandanten automatisch unterbrochen wird. Wenn Sie einen Mandanten erstellen, weist SES automatisch die Standard-Reputationsrichtlinie zu. Gehen Sie wie folgt vor, wenn Sie zu einer anderen Richtlinie wechseln möchten.

Mithilfe der Konsole:

1. Navigieren Sie in der SES-Konsole zur Seite Mandanten.
2. Wählen Sie den Mandanten aus, den Sie konfigurieren möchten.
3. Im Bereich Mandantenkonfiguration können Sie die Reputation-Richtlinienkarte verwenden, um eine Richtlinie zuzuweisen. Optional können Sie bis zum Bereich mit den Registern nach unten scrollen und die Registerkarte Reputationsrichtlinie verwenden, um dasselbe zu tun.
4. Wählen Sie eine der folgenden Richtlinien aus:

    - Standard (empfohlen) — Unterbrechen Sie den Versand, wenn Ergebnisse mit hohem Schweregrad erkannt werden.
    - Streng — Unterbricht den Versand, wenn Ergebnisse (auch mit geringem Schweregrad) festgestellt werden.
    - Keine — Unterbrechen Sie den Versand unabhängig von den Ergebnissen nicht automatisch. Mit dieser Stufe sind Risiken verbunden, wie unter beschriebenVertrauen und Sicherheit.

Mit dem AWS CLI:

```
update-reputation-entity-policy \
    --reputation-entity-type "RESOURCE" \
```

```
    --reputation-entity-reference "arn:aws:ses:us-east-1:123456789012:tenant/tenantId"
 \
    --reputation-entity-policy "arn:aws:ses:us-east-1:aws:reputation-policy/standard"
```

E-Mails mit Mietern senden

Wenn Sie E-Mails über einen Mandanten senden, müssen Sie den Mandanten in Ihren API-Aufrufen oder SMTP-Headern angeben und sicherstellen, dass alle verwendeten Ressourcen diesem Mandanten zugeordnet sind.

Themen

- Verwenden der SendEmail API mit Mandanten
- SMTP mit Mandanten verwenden

Verwenden der SendEmail API mit Mandanten

AWS CLI Beispiel:

```
aws sesv2 send-email \
  --tenant-name "MyTenant" \
  --from-email-address "sender@example.com" \
  --destination "ToAddresses=recipient@example.com" \
  --content "Simple={Subject={Data='Test Subject',Charset=utf-8},Body={Text={Data='Test
 email body',Charset=utf-8}}}" \
  --configuration-set-name "MyConfigSet"
```

AWS Beispiel für ein SDK für Python:

```
import boto3

client = boto3.client('sesv2')
response = client.send_email(
    FromEmailAddress='sender@example.com',
    Destination={
        'ToAddresses': ['recipient@example.com']
    },
    Content={
        'Simple': {
            'Subject': {
                'Data': 'Test email'
```

```
            },
            'Body': {
                'Text': {
                    'Data': 'This is a test email sent using a tenant.'
                }
            }
        }
    },
    ConfigurationSetName='MyConfigurationSet',
     TenantName='MyTenant'
)
```

SMTP mit Mandanten verwenden

Wenn Sie SMTP verwenden, um E-Mails über einen Mandanten zu senden, fügen Sie die Mandanteninformationen in einen E-Mail-Header ein:

```
X-SES-TENANT: MyTenant
```

Dieser Header teilt SES mit, welcher Mandant für den E-Mail-Versand verwendet werden soll, sodass SES die entsprechende Ressourcenvalidierung und Reputationsverfolgung durchführen kann.

Verwaltung des Mandantenstatus

Themen

- Mandantenstatus und Kennzahlen anzeigen
- Mieter pausieren und pausieren

Mandantenstatus und Kennzahlen anzeigen

Mit der Konsole:

1. Navigieren Sie in der SES-Konsole zur Seite Mandanten.
2. Wählen Sie einen Mandanten aus, um dessen Details einzusehen.
3. Im Feld Mandantenstatus wird Folgendes angezeigt:

   Sendestatus:.

   - Aktiviert — Der Mandant kann E-Mails senden.

- Pausiert — Sie oder die automatisierten Richtlinien von SES haben den Versand für diesen Mandanten angehalten.
- Durchgesetzt — SES hat den Versand aufgrund schwerwiegender Reputationsprobleme unterbrochen.
- Wieder aktiviert — Der Versand wurde nach der Unterbrechung wieder aktiviert.

Reputationsstatus:

- Keine Ergebnisse gefunden — Keine Probleme, die die Zustellbarkeit beeinträchtigen.
- Warnung mit geringem Schweregrad — Kleinere Probleme, die die Zustellbarkeit beeinträchtigen könnten, wenn sie nicht behoben werden.
- Warnung mit hohem Schweregrad — Schwerwiegende Probleme, die sich wahrscheinlich auf die Zustellbarkeit auswirken.

4. Scrollen Sie auf dem Tab Ressourcen nach unten zu Versandstatistiken, um die Statistiken zu Versand, Abmeldung und Beschwerde für den ausgewählten Zeitraum einzusehen.

Verwenden von: AWS CLI

```
# Get tenant details
aws sesv2 get-tenant --tenant-name "MyTenant"
```

Mieter pausieren und pausieren

Sie können die Sendefunktionen eines Mandanten bei Bedarf manuell unterbrechen und die Pause wieder aufheben, wenn Sie bereit sind, den Versand fortzusetzen.

Mithilfe der Konsole:

1. Navigieren Sie in der SES-Konsole zur Seite Mandanten.
2. Aktivieren Sie das Kontrollkästchen neben dem Mandanten, den Sie pausieren oder deaktivieren möchten.
3. Wählen Sie Senden unterbrechen oder Senden fortsetzen.
4. Bestätigen Sie die Aktion.

Verwenden von AWS CLI:

So pausieren Sie einen Mandanten:

```
# Pause a tenant
aws sesv2 update-reputation-entity-customer-managed-status \
  --reputation-entity-type RESOURCE
  --reputation-entity-reference "arn:aws:ses:us-east-1:593442965613:tenant/tenantId"
  --sending-status DISABLED
```

Um die Pause für einen Mandanten aufzuheben:

```
# Unpause a tenant
aws sesv2 update-reputation-entity-customer-managed-status \
  --reputation-entity-type RESOURCE
  --reputation-entity-reference "arn:aws:ses:us-east-1:593442965613:tenant/tenantId"
  --sending-status ENABLED
```

Mit Reputationsergebnissen arbeiten

Themen

- Reputationsergebnisse anzeigen
- Die Ergebnisse zur Reputation verstehen
- Lösung von Reputationsproblemen

Reputationsergebnisse anzeigen

Mithilfe der Konsole:

1. Navigieren Sie in der SES-Konsole zur Seite Mandanten.
2. Wählen Sie den Mandanten aus, den Sie untersuchen möchten.
3. Navigieren Sie zur Tabelle mit den Ergebnissen der Reputation.
4. Prüfen Sie alle aktiven Ergebnisse, einschließlich Art, Schweregrad, Erkennungsdatum und Hinweise zur Problemlösung.

Verwenden von AWS CLI:

```
aws sesv2 list-recommendations \
```

```
   --filter='{ "RESOURCE_ARN":"arn:aws:ses:us-east-1:012345678901:tenant/tenantId"}'
```

Die Antwort enthält Einzelheiten zu allen aktiven Ergebnissen:

```
{
    "Recommendations": [
        {
            "ResourceArn": "arn:aws:ses:us-east-1:012345678901:tenant/{tenant-name}/
{tenant-id}",
            "Type": "BOUNCE",
            "Description": "The bounce rate exceeded 15.0% based on a representative
 volume of 664 emails from July 11, 2025 at 14:41 (UTC) to July 11, 2025 at 16:26
 (UTC).",
            "Status": "OPEN",
            "CreatedTimestamp": "2025-07-11T16:16:14.029000+00:00",
            "LastUpdatedTimestamp": "2025-07-11T16:37:14.145000+00:00",
            "Impact": "HIGH"
        }
    ]
}
```

Die Ergebnisse zur Reputation verstehen

Die Ergebnisse zur Reputation geben Aufschluss über mögliche Probleme im Zusammenhang mit den E-Mail-Versandpraktiken Ihrer Mieter. Jedes Ergebnis beinhaltet:

- Auswirkung — Schweregrad (hoch oder niedrig).
- Art der Suche — Absprungraten, Beschwerderaten, Feedback von Drittanbietern von Postfachanbietern und IP-Sperrlisten.
- Alter — Zeit seit dem ersten Erkennungsdatum.
- Beschreibung — Kontext zum Problem (z. B. die spezifische Rate, die den Befund ausgelöst hat).
- Zuletzt überprüft — Datum der letzten Statusaktualisierung.
- Problem lösen — Links zum entsprechenden Abschnitt im SES Developer Guide mit Anleitungen zur Lösung des Problems.

Zu den häufigsten Ergebnissen gehören:

- Hohe Absprungraten — Wenn die Absprungraten die konfigurierten Schwellenwerte überschreiten.

- Beschwerdeaktivität — Wenn Spam-Berichte von Postfachanbietern eingehen, die Schwellenwerte überschreiten.
- Feedback von Drittanbietern — Negative Signale von Postfachanbietern.
- Erscheinungen auf Blocklisten — Beim Senden IPs erscheinen sie auf einer Reputations-Blockliste.

Lösung von Reputationsproblemen

Wenn Sie eine Reputationsfeststellung erhalten, ist es wichtig, die Ursache zu untersuchen und umgehend Abhilfemaßnahmen zu ergreifen:

1. Gehen Sie der Grundursache auf den Grund — Bitten Sie Ihren Mieter, die Listenhygiene zu verbessern, den E-Mail-Inhalt zu aktualisieren oder technische Probleme zu beheben.
2. Überprüfen Sie die Versandpraktiken — Stellen Sie sicher, dass Ihr Mieter die bewährten Methoden für E-Mails einhält.
3. Kennzahlen überwachen — Achten Sie auf Verbesserungen der Absprungs- und Beschwerdequoten.
4. Kommunizieren Sie mit den betroffenen Parteien — Informieren Sie die relevanten Interessengruppen über das Problem und die Lösungsschritte.

Überwachung und Analytik

Themen

- CloudWatch Metriken einrichten
- Benachrichtigungen einrichten EventBridge

CloudWatch Metriken einrichten

SES veröffentlicht mieterspezifische Kennzahlen für Amazon. CloudWatch Die folgenden Metriken sind für jeden Mandanten verfügbar:

- Sendet — Gesamtzahl der vom Mandanten gesendeten E-Mails.
- Bounces — Anzahl der zurückgesendeten E-Mails für den Mandanten.
- Beschwerden — Anzahl der zurückgesendeten E-Mails an den Mieter.

Zugriff auf Mieter-Metriken in CloudWatch:

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den AWS/SES-Namespace aus.
4. Wählen Sie Nach TenantId und TenantName, um mandantenspezifische Kennzahlen anzuzeigen.

Benachrichtigungen einrichten EventBridge

Standardmäßig sendet SES Ereignisse an den EventBridge Standardereignisbus, wenn die Reputation von Mandanten festgestellt wird oder wenn sich der Mandantenstatus ändert.

Sie können Regeln für den Standard-Event-Bus erstellen, um bestimmte Ereignisse zu identifizieren EventBridge, die dann an ein oder mehrere angegebene Ziele gesendet werden sollen.

Die folgenden Detailtypen sind verfügbar:

Für Mandanten, die Statusänderungen senden:

- `Sending Status Enabled`— Der Mandant ist aktiviert und kann E-Mails senden.
- `Sending Status Disabled`— Der Mandant wurde pausiert und kann keine E-Mails senden.

Für Reputationserkenntnisse:

- `Advisor Recommendation Status Open`
- `Advisor Recommendation Status Closed`

EventBridge Regeln aufstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Geben Sie für Ihre Regel einen Namen und eine Beschreibung ein.
4. Wählen Sie in Define pattern (Muster definieren) die Option Event pattern (Ereignismuster) aus.
5. Wählen Sie Pre-defined pattern by service (Vordefiniertes Muster nach Service)aus.

6. Wählen Sie SES als Servicenamen.
7. Wählen Sie als Ereignistyp Sendestatus aktiviert oder Sendestatus deaktiviert aus.
8. Konfigurieren Sie das Ereignismuster so, dass es bestimmten Ereignissen entspricht, an denen Sie interessiert sind.
9. Wählen Sie Ihr Ziel (z. B. eine AWS Lambda-Funktion, ein Amazon SNS SNS-Thema oder eine Amazon SQS SQS-Warteschlange).
10. Konfigurieren Sie alle zusätzlichen Einstellungen nach Bedarf.
11. Wählen Sie Erstellen aus.

Beispiel für ein EventBridge Regelmuster für Reputationsergebnisse:

```
{
  "detail-type": "Advisor Recommendation Status Open",
  "source": "aws.ses",
  "account": "012345678901",
  "time": "2023-11-15T17:00:59Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ses:us-east-1:012345678901:tenant/{tenant-name}/{tenant-id}"
  ],
  "detail": {
       "version": "1.0.0",
       "data": "The bounce rate exceeded 15.0% based on a representative volume of 197
 emails from July 11, 2025 at 14:43 (UTC) to July 11, 2025 at 16:13 (UTC).",
       "metadata":{"impact":"HIGH","type":"BOUNCE"}

    }
}
```

Beispiel für ein EventBridge Regelmuster für das Senden von Statusänderungen:

```
{
        "detail-type": "Sending Status Disabled",
        "source": "aws.ses",
        "account": "012345678901",
        "time": "2025-07-24T12:44:28Z",
        "region": "us-east-1",
        "resources": [
```

```
            "arn:aws:ses:us-east-1:012345678901:tenant/{tenant-name}/{tenant-id}"
        ],
        "detail": {
            "version": "1.0.0",
            "data": {
                "origin": "CUSTOMER_MANAGED",
                "record": {
                    "status": "DISABLED",
                    "cause": "Status manually updated.",
                    "lastUpdatedTimestamp": [2025, 7, 24, 12, 44, 28, 995000000]
                }
            }
        }
    }
```

Feldbeschreibungen:

- Quelle — Identifiziert den Dienst, der das Ereignis generiert hat. Bei SES-Ereignissen lautet dieser Wert `aws.ses`.
- detail-type — Der Typ des Statusänderungsereignisses (siehe Ereignistypen oben).
- resources — Array, das den ARN des betroffenen Mandanten enthält.
- detail.data.origin — Quelle der Statusänderung (z. B. „CUSTOMER_MANAGED“ oder "„). AWS_MANAGED
- detail.data.record.status — Der neue Status des Mandanten (AKTIVIERT, DEAKTIVIERT oder WIEDERHERGESTELLT).
- detail.data.record.cause — Beschreibung, warum sich der Status geändert hat.
- detail.data.record. lastUpdatedTimestamp — Zeitstempel, zu dem der Status aktualisiert wurde.

Sie können diese Ereignisse verwenden, um Änderungen des Mandantenstatus zu überwachen und Antworten in Ihren Anwendungen zu automatisieren. Möglicherweise möchten Sie beispielsweise Benachrichtigungen auslösen, wenn Mieter deaktiviert sind, oder die Gesundheitsdaten der Mieter im Laufe der Zeit verfolgen.

Integration mit AWS Trust & Safety

Wenn AWS Trust & Safety Probleme feststellt, die normalerweise zu einer Durchsetzung auf Kontoebene führen würden, ermöglicht das Mandantensystem gezieltere Maßnahmen. Anstatt Ihr

gesamtes Konto zu pausieren, kann Trust & Safety nur die problematischen Mandanten pausieren und gleichzeitig den gesetzeskonformen Mandanten ermöglichen, weiterhin zu senden.

Diese Durchsetzung auf Mandantenebene reduziert die Auswirkungen von Reputationsproblemen und trägt dazu bei, die Geschäftskontinuität Ihrer anderen E-Mail-Streams aufrechtzuerhalten.

Sie erhalten Benachrichtigungen, wenn SES das Senden aufgrund schwerwiegender Probleme, die sich auf die Reputation von Mietern auswirken, deaktiviert und Ihr Konto überprüft hat. Im AWS Support Center wird ein Fall für Sie geöffnet, sodass Sie mit Trust & Safety zusammenarbeiten können, um Probleme zu lösen und den Versand für den betroffenen Mandanten wiederherzustellen.

> **Note**
>
> Als Kontoinhaber liegt es in Ihrer Verantwortung, die Reputationskennzahlen all Ihrer Mieter zu überwachen. Die Mandantenfunktion isoliert zwar die Reputationsverfolgung auf Mandantenebene, aber ihre kombinierten Sendeaktivitäten wirken sich dennoch auf Ihren allgemeinen Ruf aus. Mieter, die schlechte Versandpraktiken entwickeln, könnten Ihr gesamtes Konto gefährden. Daher ist es wichtig, sicherzustellen, dass alle Mieter gute E-Mail-Versandpraktiken einhalten, um den Status Ihres Kontos zu schützen.

Best Practices

Folgen Sie diesen bewährten Methoden, um die Reputation von Mandanten in Amazon SES effektiv zu verwalten:

- Beginnen Sie mit der Standardrichtlinie — Für die meisten Mieter bietet die Standard-Reputationsrichtlinie ein ausgewogenes Verhältnis zwischen Schutz und Betriebsstabilität.
- Erst prüfen, dann durchsetzen — Wenn Sie neue Mandanten einbinden, sollten Sie in Erwägung ziehen, vorübergehend die Richtlinie „Keine“ zu verwenden und gleichzeitig deren Sendemuster (z. B. mit EventBridge) zu überwachen, bevor Sie die automatische Durchsetzung aktivieren.
- EventBridge Benachrichtigungen einrichten — Richten Sie Warnmeldungen für Reputationsfeststellungen ein, damit Sie proaktiv handeln können, bevor es zu einer automatischen Unterbrechung kommt.
- Regelmäßige Überprüfung der Mieterdaten — Überwachen Sie die Sendestatistiken auf Mandantenebene, auch wenn keine Reputationsdaten vorliegen, um neue Muster zu erkennen.
- Informieren Sie Ihre Mieter — Stellen Sie Richtlinien bereit, um Mietern Bewährte Methoden für E-Mails zu helfen, einen guten Ruf als Absender aufrechtzuerhalten.

- Wenden Sie angemessene Richtlinien an — Wenden Sie die strikte Richtlinie auf Mieter mit hohem Risiko oder auf Mieter mit Rufproblemen in der Vergangenheit an.
- Reagieren Sie schnell auf Ergebnisse — Wenn ein Befund entdeckt wird, untersuchen Sie sofort die Ursache und ergreifen Sie geeignete Abhilfemaßnahmen.
- Ressourcenplanung — Gestalten Sie Ihre Mieterstruktur so, dass sie Ihren Geschäftsanforderungen entspricht. Mieter können mehrere Kunden (ISVs), Geschäftsbereiche, client/application Typen und gesetzliche Anforderungen repräsentieren.

Einschränkungen

Beachten Sie bei der Nutzung von Tenant Management die folgenden Einschränkungen:

- Regionaler Geltungsbereich — Mandanten sind regionsspezifisch und werden nicht automatisch überall repliziert. AWS-Regionen Wenn Sie E-Mails aus mehreren Regionen versenden, müssen Sie die Mandantenreputation in jeder Region separat konfigurieren und überwachen.
- Kontingentbeschränkungen — Standardmäßig können mit Konten bis zu 10.000 Mandanten erstellt werden. Sie können Erhöhungen über die AWS Service Quota Console beantragen, wobei die automatische Genehmigung für qualifizierte Konten für bis zu 300.000 Mandanten verfügbar ist.
- Anforderung eines Konfigurationssatzes — Wenn Sie im Namen eines Mandanten senden, müssen Sie einen Konfigurationssatz angeben, der diesem Mandanten zugeordnet ist, oder eine Identität verwenden, der ein Standardkonfigurationssatz zugeordnet ist.
- Berechnungszeiträume für Metriken — Reputationsmetriken werden auf der Grundlage der letzten Sendeaktivitäten berechnet, in der Regel über einen fortlaufenden Zeitraum von 24 bis 7 Tagen, je nach Metriktyp.
- Minimales Versandvolumen — Bei einigen Reputationsergebnissen ist eine repräsentative Mindestanzahl an E-Mails erforderlich, bevor sie ausgelöst werden können.
- Kulanzzeitraum für erneute Aktivierung — Nach der erneuten Aktivierung eines angehaltenen Mandanten wird dieser in den Status „reaktiviert“ versetzt, in dem aktive Reputationserkenntnisse vorübergehend ignoriert werden, damit der Mandant sich erholen kann. Der Mandant bleibt in diesem Status, bis alle aktiven Probleme behoben sind.
- Kontoübergreifende Einschränkungen — Mandanten können sich nicht auf mehrere AWS Konten verteilen. Jedes Konto verwaltet seine eigenen Mandanten unabhängig voneinander.
- Keine Verschachtelung von Mietern — Mieter können keine anderen Mieter aufnehmen — es handelt sich um flache Gebäude.

Preisgestaltung

Je nach Anzahl der E-Mails fällt eine zusätzliche Gebühr pro Mieter und Monat an. Detaillierte Preisinformationen finden Sie auf der SES-Preisseite.

Bei Verwendung CloudWatch mit Kennzahlen für Mandanten werden die CloudWatch Standardkennzahlen für jeden Mandanten ohne zusätzliche Kosten als Teil der Basisüberwachung bereitgestellt. Für zusätzliche CloudWatch Funktionen wie benutzerdefinierte Dashboards, Alarme oder detaillierte Überwachung können CloudWatch Standardgebühren anfallen.

Verifizierte Identitäten in Amazon SES

In Amazon SES bezeichnet Identität eine E-Mail-Adresse oder eine Domäne, die Sie zum Versenden oder Empfangen von E-Mails verwenden. Bevor Sie E-Mails mit Amazon SES senden können, müssen Sie jede Identität verifizieren, die Sie als Adresse unter „From“, „Source“, „Sender“ oder „Return-Path“ verwenden werden, um nachzuweisen, dass Sie ihnen gehören. Durch Verifizierung einer Identität bei Amazon SES wird sichergestellt, dass diese Ihnen gehört, und verhindern somit eine unbefugte Nutzung.

Ist Ihr Konto noch in der Amazon SES Sandbox, müssen Sie alle E-Mail-Adressen verifizieren, an die Sie E-Mails schicken möchten, es sei denn, Sie senden an vom Amazon-SES-Postfachsimulator bereitgestellte Test-Postfächer. Weitere Informationen finden Sie unter the section called “Manuelles Verwenden des Postfachsimulators”.

Sie können eine Identität mithilfe der Amazon SES-Konsole oder der Amazon SES-API verifizieren. Der Identitätsüberprüfungsprozess hängt davon ab, welche Art von Identität Sie erstellen möchten.

> **Tip**
>
> Wenn Sie SES zum ersten Mal verwenden, können Sie den Assistenten für Erste Schritte verwenden, um Ihre erste Identität (E-Mail-Adresse oder Domain) zu erstellen und zu verifizieren.

Inhalt

- Erstellen und verifizieren von Identitäten in Amazon SES
- Verifizieren von Identitäten in Amazon SES
- Konfigurieren von Identitäten in Amazon SES
- Senden von Test-E-Mails in Amazon SES mit dem Simulator

Erstellen und verifizieren von Identitäten in Amazon SES

In Amazon SES können Sie eine Identität auf Domänenebene erstellen oder eine E-Mail-Adressidentität erstellen. Diese Identitätstypen schließen sich nicht gegenseitig aus. In den meisten Fällen entfällt durch das Erstellen einer Domänenidentität die Notwendigkeit, individuelle E-Mail-

Adressidentitäten zu erstellen und zu überprüfen, es sei denn, Sie möchten benutzerdefinierte Konfigurationen auf eine bestimmte E-Mail-Adresse anwenden. Ob Sie nun eine Domäne erstellen und E-Mail-Adressen basierend auf der Domäne verwenden oder individuelle E-Mail-Adressidentitäten erstellen – beide Ansätze bieten Vorteile. Welche Methode Sie wählen, hängt von Ihren spezifischen Bedürfnissen ab, wie unten beschrieben.

Das Erstellen und Überprüfen einer E-Mail-Adressidentität ist der schnellste Weg, um mit SES zu beginnen, aber es gibt Vorteile, eine Identität auf Domänenebene zu verifizieren. Wenn Sie eine E-Mail-Adressenidentität verifizieren, kann nur diese E-Mail-Adresse benutzt werden, um E-Mails zu versenden. Wenn Sie hingegen eine Domänenidentität verifizieren, können Sie von jeder beliebigen Subdomäne oder E-Mail-Adresse der verifizierten Domäne aus eine E-Mail senden, ohne dass diese einzeln verifiziert werden muss. Wenn Sie beispielsweise eine Domainidentität mit Namen example.com erstellen und verifizieren, müssen Sie keine separaten Subdomänenidentitäten für a.example.com, a.b.example.com oder separate E-Mail-Adressidentitäten für user@example.com, user@a.example.com usw. erstellen.

Beachten Sie jedoch, dass eine E-Mail-Adressenidentität, die die von ihrer Domain geerbte Überprüfung verwendet, auf das einfache Senden von E-Mails beschränkt ist. Wenn Sie fortgeschrittenere Sendungen durchführen möchten, müssen Sie dies auch explizit als E-Mail-Adressenidentität verifizieren. Das erweiterte Senden umfasst die Verwendung der E-Mail-Adresse mit Konfigurationssätzen, Richtlinienautorisierungen für das Senden von Delegaten und Konfigurationen, die die Domäneneinstellungen überschreiben.

Um die oben erläuterten Funktionen zur Verifizierung, Vererbung und E-Mail-Versand zu verdeutlichen, sind in der folgenden Tabelle die einzelnen Kombinationen aus domain/email Adressüberprüfung kategorisiert und jeweils die Vererbung, die Sendeebene und der Anzeigestatus aufgeführt:

	Nur Domäne verifiziert	Nur E-Mail-Adresse verifiziert	Sowohl Domäne als auch E-Mail-Adresse verifiziert
Vererbungsebene	Subdomänen und E-Mail-Adressen erben die Verifizierung von der übergeordneten Domäne.	E-Mail-Adresse wurde ausdrücklich verifiziert.	• Subdomänen erben die Verifizierung von der übergeordneten Domänen.

	Nur Domäne verifiziert	Nur E-Mail-Adresse verifiziert	Sowohl Domäne als auch E-Mail-Adresse verifiziert
			• E-Mail-Adresse wurde ausdrücklich verifiziert.
Sendeebene	E-Mail-Adressen sind auf das einfache Versenden von E-Mails beschränkt.	Die E-Mail-Adresse kann für den erweiterten Versand* verwendet werden.	Die E-Mail-Adresse kann für den erweiterten Versand* verwendet werden.
Angezeigter Status	Konsolen-/API-Status: • Domänen/Subdomänen = Verifiziert • E-Mail-Adresse = Nicht verifiziert.	Konsolen-/API-Status: • E-Mail-Adresse = Verifiziert	Konsolen-/API-Status: • Domänen/Subdomänen = Verifiziert • E-Mail-Adresse = Verifiziert.

*Der erweiterte Versand umfasst die Verwendung der E-Mail-Adresse mit Konfigurationssätzen, Richtlinienautorisierungen für das Senden von Delegaten und Konfigurationen, die die Domain-Einstellungen überschreiben.

Um E-Mails von derselben Domain oder E-Mail-Adresse in mehr als einer zu versenden AWS-Region, müssen Sie für jede Region eine eigene Identität erstellen und verifizieren. Sie können pro -Region bis zu 10.000 Identitäten verifizieren.

Beachten Sie beim Erstellen und Verifizieren von Domänen- und E-Mail-Adressidentitäten Folgendes:

- Sie können von jeder beliebigen Subdomäne oder E-Mail-Adresse der verifizierten Domäne aus eine E-Mail senden, ohne dass diese einzeln verifiziert werden muss. Wenn Sie beispielsweise eine Identität für example.com erstellen und verifizieren, müssen Sie keine separaten Identitäten für a.example.com, a.b.example.com, user@example.com, user@a.example.com usw. erstellen.
- Wie in RFC 1034 angegeben, kann jedes DNS-Label bis zu 63 Zeichen enthalten; der gesamte Domänenname darf nicht länger als 255 Zeichen sein.

- Wenn Sie eine Domäne bzw. Subdomäne oder E-Mail-Adresse mit gemeinsamer Stammdomäne verifizieren, gelten die verifizierten Identitätseinstellungen (wie Feedback-Benachrichtigungen und Easy DKIM) auf der differenziertesten der von Ihnen verifizierten Ebene.
  - Verifizierte E-Mail-Adressen-Einstellungen überschreiben verifizierte Domäneneinstellungen.
  - Verifizierte Subdomänen-Einstellungen überschreiben verifizierte Domäneneinstellungen, wobei Subdomänen-Einstellungen der unteren Ebene Subdomänen-Einstellungen der übergeordneten Ebene überschreiben.

    Beispiel: Angenommen, Sie verifizieren user@a.b.example.com, a.b.example.com, b.example.com und example.com. Dies sind die verifizierten Identitätseinstellungen, die für die folgenden Szenarien verwendet werden:
    - Für E-Mails von user@example.com (eine Adresse, die nicht explizit verifiziert wurde) werden die Einstellungen für example.com verwendet.
    - Für E-Mails von user@a.b.example.com (eine Adresse, die explizit verifiziert wurde) werden die Einstellungen für user@a.b.example.com verwendet.
    - Für E-Mails von user@b.example.com (eine Adresse, die nicht explizit verifiziert wurde) werden die Einstellungen für b.example.com verwendet.
- Sie können verifizierten E-Mail-Adressen Kennzeichen hinzufügen, ohne zusätzliche Verifizierungsschritte durchzuführen. Um einer E-Mail-Adresse ein Kennzeichen hinzufügen, fügen Sie zwischen dem Kontonamen und dem „At“-Zeichen (@) ein Pluszeichen (+) gefolgt von einem Textfeld ein. Wenn z. B. sender@example.com bereits verifiziert wurde, können Sie als Adresse unter „From“ oder „Return-Path“ für Ihre E-Mails sender+myLabel@example.com verwenden. Sie können mit dieser Funktion Variable Envelope Return Path (VERP) implementieren. Sie können mit VERP dann unzustellbare E-Mail-Adressen erkennen und aus Ihren Mailinglisten entfernen.
- Bei Domänennamen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie example.com verifizieren, können Sie Nachrichten auch von EXAMPLE.com senden.
- Bei E-Mail-Adressen ist die Groß-/Kleinschreibung relevant. Wenn Sie sender@EXAMPLE.com verifizieren, können Sie nur dann eine E-Mail von sender@example.com senden, wenn Sie auch sender@example.com verifizieren.
- In jeder AWS-Region Region können Sie bis zu 10.000 Identitäten (Domains und E-Mail-Adressen, in beliebiger Kombination) verifizieren.

> **Tip**
>
> Wenn Sie SES zum ersten Mal verwenden, können Sie den Assistenten für Erste Schritte verwenden, um Ihre erste Identität (E-Mail-Adresse oder Domain) zu erstellen und zu verifizieren.

Inhalt

- Erstellen einer Domänenidentität
- Verifizieren einer DKIM-Domänenidentität bei Ihrem DNS-Anbieter
- Erstellen einer E-Mail-Adressidentität
- Verifizieren der Identität einer E-Mail-Adresse
- Erstellen und überprüfen Sie eine Identität und weisen Sie gleichzeitig eine Standardkonfiguration zu
- Verwenden von benutzerdefinierten Vorlagen zur E-Mail-Verifizierung

Erstellen einer Domänenidentität

Ein Teil der Erstellung einer Domänenidentität ist die Konfiguration der DKIM-basierten Überprüfung. DomainKeys Identified Mail (DKIM) ist eine E-Mail-Authentifizierungsmethode, die Amazon SES verwendet, um den Domainbesitz zu verifizieren, und die empfangenden Mailserver verwenden, um die E-Mail-Authentizität zu überprüfen. Sie können DKIM entweder mit Easy DKIM oder Bring Your Own DKIM (BYODKIM) konfigurieren. Je nach Wahl müssen Sie die Signaturschlüssellänge des privaten Schlüssels wie folgt konfigurieren:

- Easy DKIM – Akzeptieren Sie entweder den Amazon-SES-Standard von 2 048 Bit oder überschreiben Sie ihn, indem Sie 1 024 Bit auswählen.
- BYODKIM – Die Länge des privaten Schlüssels muss mindestens 1024 Bits und bis zu 2048 Bit betragen.

Siehe .the section called “Länge des DKIM-Schlüssellänge”, um mehr über die DKIM-Signierung von Schlüssellängen und deren Änderung zu erfahren.

Im folgenden Verfahren wird gezeigt, wie Sie eine Domäne mithilfe der Amazon SES-Konsole erstellen.

- Wenn Sie Ihre Domäne bereits erstellt haben und sie nur verifizieren müssen, fahren Sie mit dem Verfahren the section called “Verifizieren einer Domänenidentität” auf dieser Seite fort.

So erstellen Sie eine Domänen-Identität

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie Create identity (Identität erstellen).
4. Wählen Sie unter Identity details (Identitätsdetails) -Domain (Domäne) als Identitätstyp, der erstellt werden soll. Sie müssen Zugriff auf die DNS-Einstellungen der Domäne haben, um den Domänenverifizierungsprozess abzuschließen.
5. Geben Sie den Namen der Domäne oder Subdomäne in das Feld Domain (Domäne).

   > **Tip**
   >
   > Wenn Ihre Domäne www.example.com ist, geben Sie example.com als Ihre Domäne ein. Schließen Sie nicht die „www“ ein. Wenn Sie dies tun, wird der Domänenverifizierungsprozess nicht erfolgreich sein.

6. (Optional) Wenn Sie Assiggn a default configuration set (Einen Standardkonfigurationssatz zuweisen) möchten, aktivieren Sie das Kontrollkästchen.

   1. Wählen Sie für Default configuration set (Standardkonfigurationssatz) den vorhandenen Konfigurationssatz aus, den Sie Ihrer Identität zuweisen möchten. Wenn Sie noch keine Konfigurationssätze erstellt haben, lesen Sie Konfigurationssätze.

      > **Note**
      >
      > Amazon SES wird standardmäßig nur dann der zugewiesene Konfigurationssatz verwendet, wenn zum Zeitpunkt des Sendens kein anderer Satz angegeben ist. Wenn ein Konfigurationssatz angegeben wird, wendet Amazon SES die angegebene Menge anstelle des Standardsatzes an.

7. (Optional) Wenn Sie use a custom MAIL FROM domain (Eine benutzerdefinierte MAIL-FROM-Domäne verwenden) verwenden möchten, aktivieren Sie das Kontrollkästchen, und führen Sie

die folgenden Schritte aus. Weitere Informationen finden Sie unter the section called “Verwenden einer benutzerdefinierten MAIL FROM-Domäne”.

1. Geben Sie für MAIL FROM domain (MAIL-FROM-Domäne) die Subdomäne ein, die Sie als MAIL-FROM-Domäne verwenden möchten. Es muss sich hierbei um eine Unterdomäne der Domänen-Identität handeln, die Sie verifizieren. Die MAIL FROM-Domäne sollte keine Domäne sein, von der Sie E-Mails senden.
2. FürVerhalten bei MX-Ausfall, geben Sie an, welche Aktion Amazon SES ausführen soll, wenn der erforderliche MX-Eintrag zum Zeitpunkt des Sendens nicht gefunden werden kann. Wählen Sie eine der folgenden Optionen:
   - Verwenden von region.amazonses.com als MAIL FROM-Adresse - Wenn der benutzerdefinierte MX-Eintrag der MAIL FROM-Domäne nicht ordnungsgemäß eingerichtet ist, verwendet Amazon SES eine Unterdomäne von amazonses.com. Die Unterdomäne variiert je nach der AWS-Region -Region, in der Sie Amazon SES verwenden.
   - Nachricht ablehnen – Wenn ein benutzerdefinierter MX-Eintrag der MAIL FROM-Domäne nicht ordnungsgemäß eingerichtet ist, gibt Amazon SES einen `MailFromDomainNotVerified`-Fehler zurück. E-Mails, die Sie von dieser Domäne aus senden möchten, werden automatisch abgelehnt.
3. Wenn Ihre Domäne über Amazon Route 53 gehostet wird, haben Sie für Veröffentlichen von DNS-Datensätzen in Route53 die Möglichkeit, SES die zugehörigen TXT- und MX-Datensätze zum Zeitpunkt der Erstellung veröffentlichen zu lassen, indem Sie Aktiviert aktiviert lassen. Wenn Sie diese Datensätze lieber später veröffentlichen möchten, deaktivieren Sie das Kontrollkästchen Enabled (Aktiviert). (Sie können zu einem späteren Zeitpunkt zurückkehren, um die Datensätze auf Route 53 zu veröffentlichen, indem Sie die Identität bearbeiten – siehe the section called “Bearbeiten Sie eine Identität mit der Konsole”.)

8. (Optional) Um eine benutzerdefinierte DKIM-basierte Überprüfung zu konfigurieren, die nicht die SES-Standardeinstellung verwendet, bei der Easy DKIM mit einer Signaturlänge von 2048 Bit verwendet wird, erweitern Sie unter Domain verifizieren den Bereich Erweiterte DKIM-Einstellungen und wählen Sie den DKIM-Typ aus, den Sie konfigurieren möchten:

   a. Easy DKIM:

      i. Wählen Sie unter Identitätstyp die Option Easy DKIM aus.

      ii. Im Feld DKIM signing key length (Länge des DKIM-Signierschlüssels), wählen Sie entweder RSA_2048_BIT oder RSA_1024_BIT aus.

iii. Wenn Ihre Domäne über Amazon Route 53 gehostet wird, haben Sie für Veröffentlichen von DNS-Datensätzen in Route53 die Möglichkeit, SES die zugehörigen CNAME-Datensätze zum Zeitpunkt der Erstellung veröffentlichen zu lassen, indem Sie Enabled (Aktiviert) aktiviert lassen. Wenn Sie diese Datensätze lieber später veröffentlichen möchten, deaktivieren Sie das Kontrollkästchen Enabled (Aktiviert). (Sie können zu einem späteren Zeitpunkt zurückkehren, um die Datensätze auf Route 53 zu veröffentlichen, indem Sie die Identität bearbeiten – siehe the section called “Bearbeiten Sie eine Identität mit der Konsole”.)

b. Deterministisches Easy DKIM (DEED):

> **Tip**
>
> Diese Form von DKIM sollte verwendet werden, wenn Sie eine globale (Replikat-) Identität erstellen. DEED verwendet das einfache DKIM-Setup einer vorhandenen Identität mit demselben Namen aus einer übergeordneten Region und signiert die neue Identität, ohne dass Sie eine zusätzliche DNS-Einrichtung durchführen müssen. Weitere Informationen finden Sie unter DEED.

i. Wählen Sie unter Identitätstyp die Option Deterministic Easy DKIM aus.

ii. Wählen Sie im Dropdownmenü Übergeordnete Region eine übergeordnete Region aus, in der sich eine von Easy DKIM signierte Identität mit demselben Namen befindet, den Sie für Ihre globale (Replikat-) Identität eingegeben haben. (Ihre Replikatregion ist standardmäßig die Region, mit der Sie sich bei der SES-Konsole angemeldet haben.)

c. DKIM-Authentifizierungstoken bereitstellen (BYODKIM):

i. Stellen Sie sicher, dass Sie bereits ein öffentlich-privates Schlüsselpaar generiert und den öffentlichen Schlüssel zu Ihrem DNS-Host-Anbieter hinzugefügt haben. Weitere Informationen finden Sie unter the section called “BYODKIM - Verwendung Ihrer eigenen DKIM”.

ii. Wählen Sie unter Identitätstyp die Option DKIM-Authentifizierungstoken bereitstellen (BYODKIM) aus.

iii. Für Privater Aktivierungsschlüssel fügen Sie den privaten Schlüssel ein, den Sie aus Ihrem öffentlich-privaten Schlüsselpaar generiert haben. Der private Schlüssel muss mindestens 1024-Bit-RSA-Verschlüsselung und bis zu 2048-Bit verwenden und mit base64-Codierung (PEM) codiert werden.

> **Note**
>
> Sie müssen die erste und letzte Zeile (`-----BEGIN PRIVATE KEY-----` bzw. `-----END PRIVATE KEY-----`) des generierten privaten Schlüssels löschen. Darüber hinaus müssen Sie die Zeilenumbrüche im generierten privaten Schlüssel entfernen. Der resultierende Wert ist eine Zeichenfolge ohne Leerzeichen oder Zeilenumbrüche.

iv. Geben Sie für Selector name (Name des Selektors) den Namen des Selektors ein, der in den DNS-Einstellungen Ihrer Domäne angegeben werden soll.

9. Stellen Sie sicher, dass die Enabled (Aktiviert) ist im FeldDKIM signatures (DKIM-Signaturen).
10. (Optional) Fügen Sie mindestens einen Tags zu Ihrer Domänenidentität hinzufügen, indem Sie einen Tag-Schlüssel und einen optionalen Wert für den Schlüssel einschließen:
    1. Klicken Sie auf Add new tag (Neues Tag hinzufügen) und geben Sie die Key (Schlüssel) aus. Sie können einen optionalen Wert für das Tag unter Value (Wert) hinzufügen.
    2. Wiederholen Sie diesen Vorgang für zusätzliche Tags, die 50 nicht überschreiten, oder wählen Sie Remove (Entfernen), um die Tags zu entfernen.
11. Wählen Sie Create identity (Identität erstellen).

Nachdem Sie nun Ihre Domänenidentität mit DKIM erstellt und konfiguriert haben, müssen Sie den Verifizierungsprozess bei Ihrem DNS-Anbieter abschließen – fahren Sie mit the section called “Verifizieren einer Domänenidentität” fort und befolgen Sie die DNS-Authentifizierungsverfahren für den DKIM-Typ, mit dem Ihre Identität konfiguriert wurde.

> **Note**

Verifizieren einer DKIM-Domänenidentität bei Ihrem DNS-Anbieter

Nachdem Sie Ihre mit DKIM konfigurierte Domänenidentität erstellt haben, müssen Sie den Überprüfungsprozess bei Ihrem DNS-Anbieter abschließen, indem Sie die entsprechenden Authentifizierungsverfahren für den von Ihnen gewählten DKIM-Typ befolgen.

Wenn Sie noch keine Domänenidentität erstellt haben, informieren Sie sich unter the section called “Erstellen einer Domänenidentität”.

> **Note**
>
> - Das Überprüfen einer Domänenidentität erfordert Zugriff auf die DNS-Einstellungen der Domäne. Die Weitergabe von Änderungen an diesen Einstellungen kann bis zu 72 Stunden in Anspruch nehmen.
> - Wenn Sie mit Deterministic Easy DKIM (DEED) eine globale (replizierte) Identität erstellt haben, ist keine zusätzliche DNS-Einrichtung erforderlich. Sie können diesen Schritt überspringen. Weitere Informationen finden Sie unter DEED.

So überprüfen Sie eine DKIM-Domänenidentität bei Ihrem DNS-Anbieter

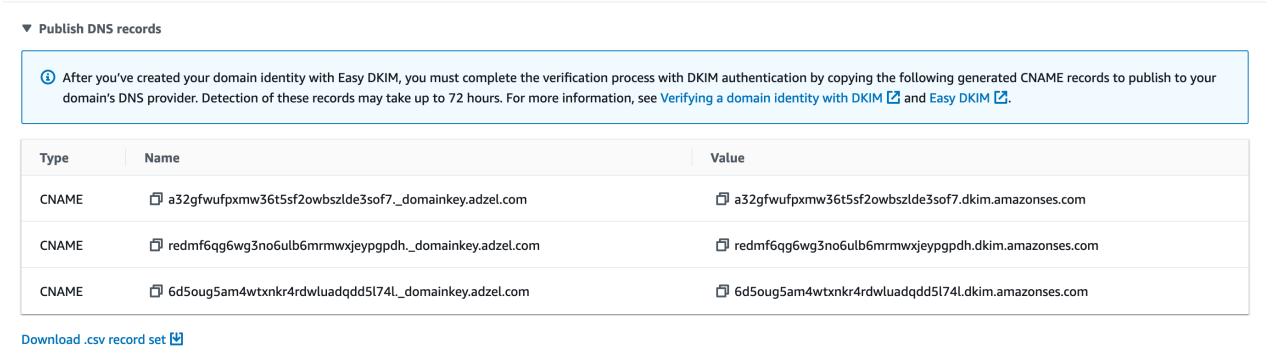
1. Wählen Sie in der Tabelle Loaded identities (Geladene Identitäten) die Domäne aus, die Sie überprüfen möchten.
2. Erweitern Sie auf der Registerkarte Authentication (Authentifizierung) der Seite „Identity details“ (Identitätsdetails) die Option Publish DNS records (DNS-Datensätze veröffentlichen).
3. Je nachdem, mit welcher DKIM-Variante Sie Ihre Domäne konfiguriert haben, Easy DKIM oder BYODKIM, folgen Sie den jeweiligen Anweisungen:

   Easy DKIM

   So verifizieren Sie eine mit Easy DKIM konfigurierte Domäne

   1. Kopieren Sie aus der Tabelle Publish DNS records (DNS-Datensätze veröffentlichen) die drei CNAME-Datensätze, die in diesem Abschnitt angezeigt werden, damit sie an Ihren DNS-Anbieter veröffentlicht (ihm hinzugefügt) werden. Alternativ können Sie Download Record Set as CSV (Datensatz als CSV-Datei herunterladen) auswählen, um eine Kopie der Datensätze auf Ihrem Computer zu speichern.

      Die folgende Abbildung enthält ein Beispiel für CNAME-Datensätze, die Sie an Ihren DNS-Anbieter veröffentlichen möchten.



2. Fügen Sie die CNAME-Datensätze den DNS-Einstellungen Ihrer Domäne entsprechend Ihrem DNS-Hostanbieter hinzu:

   - Alle DNS-Host-Anbieter (mit Ausnahme von Route 53) – Melden Sie sich bei dem DNS- oder Webhosting-Anbieter Ihrer Domäne an und fügen Sie dann die CNAME-Datensätze hinzu, die die Werte enthalten, die Sie zuvor kopiert oder gespeichert haben. Verschiedene Anbieter nutzen unterschiedliche Verfahren zum Aktualisieren von DNS-Datensätzen. Siehe die DNS/Hosting-Anbieter-Tabelle im Anschluss an diese Verfahren.

     > **Note**
     >
     > Einige wenige DNS-Anbieter lassen keine Unterstriche (_) in den Namen von Datensätzen zu. Der Unterstrich im DKIM-Datensatznamen ist jedoch erforderlich. Wenn Ihr DNS-Anbieter keine Unterstriche im Datensatznamen zulässt, bitten Sie das Kundensupport-Team des Anbieters um Hilfe.

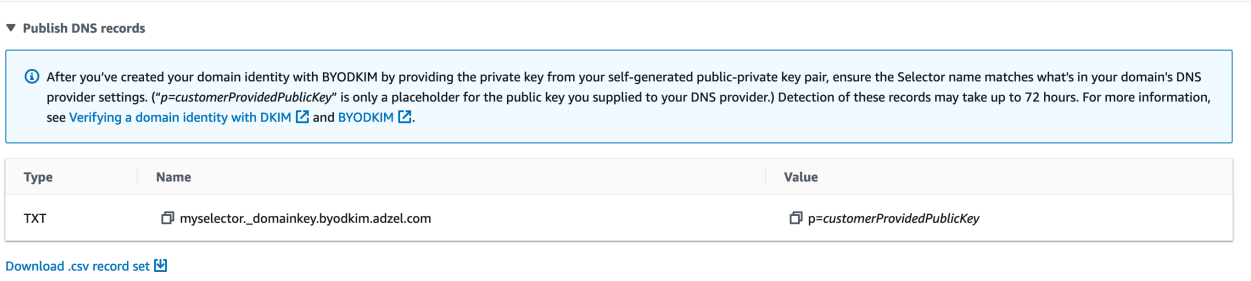
   - Route 53 als Ihr DNS-Hostanbieter – Wenn Sie Route 53 für dasselbe Konto verwenden, das Sie beim Senden von E-Mails mit SES verwenden, wählen Sie SES, um automatisch die DNS-Einstellungen für Ihre Domäne zu aktualisieren, wenn Sie zum Zeitpunkt des Erstellens aktiviert haben, dass SES sie veröffentlicht. Andernfalls können Sie sie nach der Erstellung einfach mit einem Klick auf Route 53 veröffentlichen – siehe dafür the section called “Bearbeiten Sie eine Identität mit der Konsole”. Wenn Ihre DNS-Einstellungen nicht automatisch aktualisiert werden oder Sie CNAME-Einträge zu Route 53 hinzufügen möchten, die sich nicht auf demselben Konto befinden, das Sie beim Senden von E-Mails mit SES verwenden, führen Sie die unter Editing records (Datensätze bearbeiten) beschriebenen Verfahren aus.
   - Wenn Sie nicht wissen, wer Ihr DNS-Anbieter ist - Fragen Sie Ihren Systemadministrator nach dem DNS-Anbieter.

BYODKIM

So verifizieren Sie eine mit BYODKIM konfigurierte Domäne

1. Als Sie Ihre Domäne mit BYODKIM erstellt oder eine bestehende Domäne mit BYODKIM konfiguriert haben, haben Sie das Präfix für den privaten Schlüssel (aus Ihrem selbst generierten Schlüsselpaar aus öffentlichem und privatem Schlüssel) und den Selektornamen in die entsprechenden Felder auf der Seite „Advance DKIM Settings“ (Erweiterte DKIM-Einstellungen) der SES-Konsole eingefügt. Sie müssen jetzt den Überprüfungsprozess abschließen, indem Sie die folgenden Datensätze für Ihren DNS-Host-Anbieter aktualisieren.
2. Kopieren Sie aus der Tabelle Publish DNS records (DNS-Datensätze veröffentlichen) den Datensatz des Selektornamens, der in der Spalte Name angezeigt wird, damit er an Ihren DNS-Anbieter veröffentlicht (ihm hinzugefügt) wird. Alternativ können Sie Download Record Set as CSV (Datensatz als CSV-Datei herunterladen) auswählen, um eine Kopie auf Ihrem Computer zu speichern.

   Die folgende Abbildung enthält ein Beispiel für den Datensatz des Selektornamens, den Sie an Ihren DNS-Anbieter veröffentlichen möchten.



3. Melden Sie sich bei dem DNS- oder Webhosting-Anbieter Ihrer Domäne an und fügen Sie dann den Datensatz hinzu, den Sie zuvor kopiert oder gespeichert haben. Verschiedene Anbieter nutzen unterschiedliche Verfahren zum Aktualisieren von DNS-Datensätzen. Siehe die DNS/Hosting-Anbieter-Tabelle im Anschluss an diese Verfahren.

> **Note**
>
> Einige wenige DNS-Anbieter lassen keine Unterstriche (_) in den Namen von Datensätzen zu. Der Unterstrich im DKIM-Datensatznamen ist jedoch

erforderlich. Wenn Ihr DNS-Anbieter keine Unterstriche im Datensatznamen zulässt, bitten Sie das Kundensupport-Team des Anbieters um Hilfe.

4. Wenn Sie dies noch nicht getan haben, fügen Sie dem DNS- oder Webhosting-Anbieter Ihrer Domäne den öffentlichen Schlüssel aus Ihrem selbst generierten Schlüsselpaar aus öffentlichem und privatem Schlüssel hinzu.

   Beachten Sie, dass in der Tabelle DNS-Einträge veröffentlichen der Eintrag mit dem öffentlichen Schlüssel, der in der Spalte Wert angezeigt wird, nur „p= customerProvidedPublicKey“ als Platzhalter für den Wert des öffentlichen Schlüssels anzeigt, den Sie auf Ihrem Computer gespeichert oder Ihrem DNS-Anbieter zur Verfügung gestellt haben.

   > **Note**
   >
   > Wenn Sie Ihren öffentlichen Schlüssel an Ihren DNS-Anbieter veröffentlichen (ihm hinzufügen), muss er wie folgt formatiert sein:
   >
   > - Sie müssen die erste und letzte Zeile (`-----BEGIN PUBLIC KEY-----` bzw. `-----END PUBLIC KEY-----`) des generierten öffentlichen Schlüssels löschen. Darüber hinaus müssen Sie die Zeilenumbrüche im generierten öffentlichen Schlüssel entfernen. Der resultierende Wert ist eine Zeichenfolge ohne Leerzeichen oder Zeilenumbrüche.
   > - Sie müssen das Präfix p=, wie in der Spalte Value (Wert) der Tabelle Publish DNS records (DNS-Datensätze veröffentlichen) gezeigt, einschließen.

> **Tip**
>
> Gehen Sie beim Hinzufügen von CNAME-Einträgen zu Ihrer DNS-Konfiguration wie folgt vor:
>
> - Verwenden Sie die exakten Datensatznamen, wie sie in der SES-Konsole angegeben sind.
> - Fügen Sie am Anfang der CNAME-Datensatznamen keine zusätzlichen Unterstriche (_) hinzu.

- Der `_domainkey` Teil ist Teil des Datensatznamens und sollte genau wie abgebildet verwendet werden.

Beispiel, das die korrekte und die falsche Implementierung eines CNAME-Eintrags zeigt:

- Richtig: `abc123._domainkey.domain.com`
- Falsch: `_abc123._domainkey.domain.com`

4. Es kann bis zu 72 Stunden dauern, bis Änderungen an den DNS-Einstellungen weitergegeben werden. Sobald Amazon SES alle dieser DKIM-Einträge in der DNS-Konfiguration Ihrer Domäne erkennt, ist der Überprüfungsprozess abgeschlossen. Die DKIM configuration (DKIM-Konfiguration) wird als SUCCESund Status wird als Verified (Bestätigt) aus.
5. Wenn Sie eine benutzerdefinierte MAIL FROM-Domäne konfigurieren und überprüfen möchten, folgen Sie den Verfahren unter Konfigurieren Ihrer benutzerdefinierten MAIL-FROM-Domain.

Die folgende Tabelle enthält Links zur Dokumentation für einige gängige DNS-Anbieter. Diese Liste ist nicht vollständig und stellt keine Empfehlung dar. Wenn Ihr DNS-Anbieter nicht aufgeführt ist, bedeutet dies nicht, dass Sie die Domäne nicht mit Amazon SES verwenden können.

DNS/Hosting-Anbieter	Link zur Dokumentation
GoDaddy	Einen CNAME-Datensatz hinzufügen (externer Link)
DreamHost	Wie füge ich benutzerdefinierte DNS-Daten sätze hinzu? (externer Link)
Cloudflare	Verwalten von DNS-Datensätzen in CloudFlare (externer Link)
HostGator	DNS-Einträge mit HostGator /eNom verwalten (externer Link)
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC Einträge für meine Domain hinzu? (externer Link)

DNS/Hosting-Anbieter	Link zur Dokumentation
Names.co.uk	Ändern der DNS-Einstellungen Ihrer Domänen (externer Link)
Wix	Hinzufügen oder Aktualisieren von CNAME-Datensätzen in Ihrem Wix-Konto (externer Link)

Fehlerbehebung bei der Domänenverifizierung

Wenn Sie die vorhergehenden Schritte ausgeführt haben, Ihre Domäne jedoch nach 72 Stunden noch nicht überprüft wurde, überprüfen Sie Folgendes:

- Stellen Sie sicher, dass Sie die Werte für die DNS-Einträge in die richtigen Felder eingegeben haben. Einige DNS-Anbieter bezeichnen das Feld Name/host (Name/Host) als Host oder Hostname. Darüber hinaus wird das Feld Record value (Datensatzwert) von einigen Anbietern als Points to (Verweist auf) oder Result (Ergebnis) bezeichnet.
- Stellen Sie sicher, dass Ihr Anbieter Ihren Domänennamen nicht automatisch an das Ende des Werts Name/Host, den Sie im DNS-Datensatz eingegeben haben, anhängt hat. Einige Anbieter fügen den Domänennamen an, ohne darauf hinzuweisen. Wenn Ihr Anbieter Ihren Domänennamen an das Ende des Werts Name/host (Name/Host) angefügt hat, entfernen Sie den Domänennamen vom Ende des Werts. Sie können auch einen Punkt an das Ende des Werts im DNS-Datensatz setzen. Dieser Punkt teilt dem Anbieter mit, dass der Domänenname vollständig qualifiziert ist.
- Der Unterstrich (_) ist im Wert Name/host (Name/Host) jedes DNS-Datensatzes erforderlich. Wenn Ihr Anbieter keine Unterstriche in DNS-Datensatznamen zulässt, wenden Sie sich an den Kundensupport des Anbieters, um weitere Unterstützung zu erhalten.
- Die Validierungsdatensätze, die Sie zu den DNS-Einstellungen Ihrer Domain hinzufügen müssen, sind jeweils unterschiedlich AWS-Region. Wenn Sie eine Domain verwenden möchten, um E-Mails von mehreren zu versenden AWS-Regionen, müssen Sie für jede dieser Regionen eine separate Domain-Identität erstellen und verifizieren.

Erstellen einer E-Mail-Adressidentität

Führen Sie die Schritte in diesem Abschnitt aus, um mithilfe der Amazon-SES-Konsole eine Identität für eine E-Mail-Adresse zu erstellen.

Erstellen einer E-Mail-Adressenidentität (Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie Create identity (Identität erstellen).
4. Wählen Sie unter Identity details (Identitätsdetails) Email address (E-Mail-Adresse) als Identitätstyp, der erstellt werden soll.
5. Geben Sie für Email address (E-Mail-Adresse) die E-Mail-Adresse ein, die Sie verifizieren möchten. Die E-Mail-Adresse muss eine Adresse sein, auf die Sie zugreifen können und die E-Mails empfangen kann.
6. (Optional) Wenn Sie Assiggn a default configuration set (Einen Standardkonfigurationssatz zuweisen) möchten, aktivieren Sie das Kontrollkästchen.

   1. Wählen Sie für Default configuration set (Standardkonfigurationssatz) den vorhandenen Konfigurationssatz aus, den Sie Ihrer Identität zuweisen möchten. Wenn Sie noch keine Konfigurationssätze erstellt haben, lesen Sie Konfigurationssätze.

      > **Note**
      >
      > Amazon SES wird standardmäßig nur dann der zugewiesene Konfigurationssatz verwendet, wenn zum Zeitpunkt des Sendens kein anderer Satz angegeben ist. Wenn ein Konfigurationssatz angegeben wird, wendet Amazon SES die angegebene Menge anstelle des Standardsatzes an.

7. (Optional) Fügen Sie mindestens einen Tags zu Ihrer Domänenidentität hinzufügen, indem Sie einen Tag-Schlüssel und einen optionalen Wert für den Schlüssel einschließen:

   1. Klicken Sie auf Add new tag (Neues Tag hinzufügen) und geben Sie die Key (Schlüssel) aus. Sie können einen optionalen Wert für das Tag unter Value (Wert) hinzufügen.
   2. Wiederholen Sie diesen Vorgang für zusätzliche Tags, die 50 nicht überschreiten, oder wählen Sie Remove (Entfernen), um die Tags zu entfernen.
8. Um Ihre E-Mail-Adressenidentität zu erstellen, wählen Sie Create identity (Identität erstellen) aus. Wenn Sie erstellt haben, erhalten Sie innerhalb von fünf Minuten eine Bestätigungs-E-Mail. Der nächste Schritt besteht darin, Ihre E-Mail-Adresse zu verifizieren, indem Sie die Überprüfung im nächsten Abschnitt befolgen.

> **Note**
>
> Sie können die Nachrichten anpassen, die an die zu verifizierenden E-Mail-Adressen gesendet werden. Weitere Informationen finden Sie unter the section called “Verwenden von benutzerdefinierten Vorlagen zur E-Mail-Verifizierung”.

Nachdem Sie nun die Identität für Ihre E-Mail-Adresse erstellt haben, müssen Sie den Verifizierungsprozess abschließen – fahren Sie mit the section called “Verifizieren der Identität einer E-Mail-Adresse” fort.

Verifizieren der Identität einer E-Mail-Adresse

Nachdem Sie die Identität Ihrer E-Mail-Adresse erstellt haben, müssen Sie den Verifizierungsprozess abschließen.

Wenn Sie noch keine Identität für Ihre E-Mail-Adresse erstellt haben, informieren Sie sich unter the section called “Erstellen einer E-Mail-Adressidentität”.

So verifizieren Sie die Identität einer E-Mail-Adresse

1. Überprüfen Sie den Posteingang der E-Mail-Adresse, mit der Sie Ihre Identität erstellt haben, und suchen Sie nach einer E-Mail von no-reply-aws @amazon .com.
2. Öffnen Sie die E-Mail und klicken Sie auf den Link in der E-Mail, um die Verifizierung der E-Mail-Adresse abzuschließen. Nachdem es abgeschlossen ist, wird Status auf Verified (Bestätigt) aktualisiert.

Fehlerbehebung bei der Verifizierung der E-Mail-Adresse

Wenn Sie die Verifizierungs-E-Mail nicht innerhalb von fünf Minuten nach dem Erstellen Ihrer Identität erhalten, führen Sie die folgenden Schritte zur Fehlerbehebung durch:

- Stellen Sie sicher, dass Sie die Adresse richtig eingegeben haben.
- Stellen Sie sicher, dass die E-Mail-Adresse, die Sie bestätigen möchten, E-Mails empfangen kann. Sie können dies testen, indem Sie eine andere E-Mail-Adresse verwenden, um eine Test-E-Mail an die zu bestätigende Adresse zu senden.
- Überprüfen Sie Ihren Junk-Mail-Ordner.

- Der Link in der Bestätigungs-E-Mail läuft nach 24 Stunden ab. Um eine neue Bestätigungs-E-Mail zu senden, wählen Sie Resend (Erneut senden) oben auf der Seite mit Identitätsdetails.

Erstellen und überprüfen Sie eine Identität und weisen Sie gleichzeitig eine Standardkonfiguration zu

Sie können den CreateEmailIdentityVorgang in der Amazon SES API v2 verwenden, um eine neue E-Mail-Identität zu erstellen und gleichzeitig deren Standardkonfiguration festzulegen.

> **Note**
>
> Bevor Sie die Verfahren in diesem Abschnitt abschließen, müssen Sie zunächst die AWS CLI installieren und konfigurieren. Weitere Informationen finden Sie im AWS Command Line Interface -Benutzerhandbuch.

Um einen Standardkonfigurationssatz festzulegen, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile den folgenden Befehl ein, um den CreateEmailIdentityVorgang zu verwenden.

```
aws sesv2 create-email-identity --email-identity ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Ersetzen Sie es in den vorherigen Befehlen *ADDRESS-OR-DOMAIN* durch die E-Mail-Identität, die Sie überprüfen möchten. *CONFIG-SET*Ersetzen Sie es durch den Namen des Konfigurationssatzes, den Sie als Standardkonfigurationssatz für die Identität festlegen möchten.

Bei erfolgreicher Ausführung wird der Befehl ohne Ausgabe beendet.

So verifizieren Sie Ihre E-Mail-Adresse

1. Überprüfen Sie den Posteingang der von Ihnen verifizierten E-Mail-Adresse. Sie erhalten eine Nachricht mit der folgenden Betreffzeile: „Amazon Web Services — Anfrage zur Überprüfung der E-Mail-Adresse in der Region“*RegionName*, wobei der Name der Person angegeben *RegionName* ist AWS-Region , in der Sie versucht haben, die E-Mail-Adresse zu verifizieren.

   Öffnen Sie die Nachricht, und klicken Sie dann auf den darin enthaltenen Link.

> **Note**
>
> Der Link in der Verifizierungsnachricht läuft 24 Stunden nach dem Senden der Nachricht ab. Wenn seit dem Eingang der Verifizierungs-E-Mail 24 Stunden vergangen sind, wiederholen Sie die Schritte 1 bis 5, um eine Verifizierungs-E-Mail mit einem gültigen Link zu erhalten.

2. Wählen Sie in der Amazon-SES-Konsole unter Identity Management (Identitätsmanagement) die Option Email Addresses (Email-Adressen). Suchen Sie in der Liste der E-Mail-Adressen die E-Mail-Adresse, die Sie verifizieren möchten. Wenn die E-Mail-Adresse verifiziert wurde, lautet der Wert in der Spalte Status „verified“ (bestätigt).

Um Ihre Domäne zu verifizieren

Wenn Sie im oben beschriebenen Befehlszeilenverfahren einen Domainnamen für den Parameter `--email-identity` eingegeben haben, finden Sie unter Verifizieren einer Domänenidentität weitere Informationen.

Verwenden von benutzerdefinierten Vorlagen zur E-Mail-Verifizierung

Wenn Sie versuchen, eine E-Mail-Adresse zu verifizieren, sendet Amazon SES eine E-Mail an diese Adresse, ähnlich dem Beispiel in der folgenden Abbildung.

Dear Amazon Web Services Customer,

We have received a request to authorize this email address for use with Amazon SES and Amazon Pinpoint in region US West (Oregon). If you requested this verification, please go to the following URL to confirm that you are authorized to use this email address:

https://email-verification.us-west-2.amazonaws.com/?AWSAccessKeyId=AKIADQKE4EXAMPLE&Context=109876543210&Identity.IdentityName=recipient%40example.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=TJDufFhYYK1fSHCSBq4cjbodBQq%2FnyyZgzjqZ%2BXsDYEXAMPLE&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2017-12-06T19%3A53%3A12.311Z

Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification request.

If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phishing attempt, but either a misunderstanding of how to use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully communicated the procedure first. If you are still concerned, please forward this notification to aws-email-domain-verification@amazon.com and let us know in the forward that you did not request the verification.

To learn more about sending email from Amazon Web Services, please refer to the Amazon SES Developer Guide at http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html and Amazon Pinpoint Developer Guide at http://docs.aws.amazon.com/pinpoint/latest/userguide/welcome.html.

Sincerely,

The Amazon Web Services Team.

Mehrere Amazon SES-Kunden erstellen Anwendungen (wie E-Mail-Marketing-Pakete oder Ticketing-Systeme), die E-Mails über Amazon SES im Namen ihrer eigenen Kunden senden. Für die Endbenutzer dieser Anwendungen kann die E-Mail-Verifizierung verwirrend sein: Die Verifizierungs-E-Mail verwendet Amazon SES-Branding und nicht das Branding der Anwendung und diese Endbenutzer haben sich nie angemeldet, um Amazon SES direkt zu verwenden.

Wenn Ihr Amazon SES-Anwendungsfall erfordert, dass Ihre Kunden ihre E-Mail-Adressen für eine Nutzung mit Amazon SES überprüfen lassen, können Sie benutzerdefinierte Verifizierungs-E-Mails erstellen. Diese angepassten E-Mails reduzieren die Kundenverwirrung und erhöhen die Raten, mit denen Ihre Kunden die Registrierung abschließen.

> **Note**
>
> Um diese Funktion nutzen zu können, muss sich Ihr Amazon SES-Konto außerhalb der Sandbox befinden. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).

Themen in diesem Abschnitt:

- Erstellen einer benutzerdefinierten Vorlage zur E-Mail-Verifizierung
- Bearbeiten einer benutzerdefinierten Vorlage zur E-Mail-Verifizierung
- Senden von Verifizierungs-E-Mails mit benutzerdefinierten Vorlagen
- Benutzerdefinierte Verifizierungs-E-Mail – Häufig gestellte Fragen

Erstellen einer benutzerdefinierten Vorlage zur E-Mail-Verifizierung

Um eine benutzerdefinierte Verifizierungs-E-Mail zu erstellen, verwenden Sie die `CreateCustomVerificationEmailTemplate`-API-Operation. Diese Operation akzeptiert die folgenden Eingaben:

Attribut	Description
`TemplateName`	Der Name der Vorlage. Der angegebene Name muss eindeutig sein.
`FromEmailAddress`	Die E-Mail-Adresse, von der die Verifizierungs-E-Mail gesendet wird. Die angegebene Adresse oder Domäne muss für die Verwendung mit Ihrem Amazon SES-Konto überprüft werden.

Attribut	Description
	Note Das `FromEmailAddress` -Attribut unterstützt keine Anzeigenamen (auch bekannt als "friendly from"-Namen).
`TemplateSubject`	Die Betreffzeile der Verifizierungs-E-Mail.
`TemplateContent`	Der Text der E-Mail. Der E-Mail-Text kann HTML mit bestimmten Beschränkungen enthalten. Weitere Informationen finden Sie unter Benutzerdefinierte Verifizierungs-E-Mail – Häufig gestellte Fragen.
`SuccessRedirectionURL`	Die URL, die Benutzern gesendet wird, wenn deren E-Mail-Adressen erfolgreich überprüft werden.
`FailureRedirectionURL`	Die URL, die Benutzern gesendet wird, wenn deren E-Mail-Adressen nicht erfolgreich überprüft werden.

Sie können das AWS SDKs oder verwenden AWS CLI , um im Rahmen des `CreateCustomVerificationEmailTemplate` Vorgangs eine benutzerdefinierte E-Mail-Vorlage für die Bestätigung zu erstellen. Weitere Informationen zu finden Sie AWS SDKs unter Tools für Amazon Web Services. Weitere Informationen zu finden Sie AWS CLI unter AWS Befehlszeilenschnittstelle.

Der folgende Abschnitt enthält Verfahren zum Erstellen einer benutzerdefinierten Verifizierungs-E-Mail mit der AWS CLI. Diese Verfahren setzen voraus, dass Sie die AWS CLI bereits installiert und konfiguriert haben. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Note

Um das Verfahren in diesem Abschnitt abzuschließen, müssen Sie Version 1.14.6 oder höher der AWS CLI verwenden. Um die besten Ergebnisse zu erzielen, führen Sie ein Upgrade auf die neueste Version der AWS CLI aus. Weitere Informationen zur Aktualisierung von finden Sie unter Installation von AWS Command Line Interface im AWS Command Line Interface Benutzerhandbuch. AWS CLI

1. Erstellen Sie in einem Texteditor eine neue Datei. Fügen Sie folgenden Inhalt in den Editor ein:

```
{
  "TemplateName": "SampleTemplate",
  "FromEmailAddress": "sender@example.com",
  "TemplateSubject": "Please confirm your email address",
  "TemplateContent": "<html>
                      <head></head>
                      <body style='font-family:sans-serif;'>
                        <h1 style='text-align:center'>Ready to start sending
                        email with ProductName?</h1>
                        <p>We here at Example Corp are happy to have you on
                          board! There's just one last step to complete before
                          you can start sending email. Just click the following
                          link to verify your email address. Once we confirm that
                          you're really you, we'll give you some additional
                          information to help you get started with ProductName.</p>
                      </body>
                      </html>",
  "SuccessRedirectionURL": "https://www.example.com/verifysuccess",
  "FailureRedirectionURL": "https://www.example.com/verifyfailure"
}
```

> **Important**
>
> Damit das vorherige Beispiel besser lesbar ist, enthält das `TemplateContent`-Attribut Zeilenumbrüche. Wenn Sie das vorherige Beispiel in Ihre Textdatei einfügen, entfernen Sie die Zeilenumbrüche, bevor Sie fortfahren.

Ersetzen Sie die Werte von `TemplateName`, `FromEmailAddress`, `TemplateSubject`, `TemplateContent`, `SuccessRedirectionURL` und `FailureRedirectionURL` mit Ihren eigenen Werten.

> **Note**
>
> Die E-Mail-Adresse, die Sie für das`FromEmailAddress`-Parameter angeben, muss verifiziert sein, oder es muss sich um eine Adresse in einer verifizierten Domäne handeln. Weitere Informationen finden Sie unter Verifizierte Identitäten in Amazon SES.

Wenn Sie fertig sind, speichern Sie die Datei unter `customverificationemail.json`.

2. Geben Sie in der Befehlszeile den folgenden Befehl ein, um eine benutzerdefinierte Verifizierungs-E-Mail-Vorlage zu erstellen:

```
aws sesv2 create-custom-verification-email-template --cli-input-json file://
customverificationemail.json
```

3. Optional können Sie bestätigen, dass die Vorlage erstellt wurde, indem Sie den folgenden Befehl eingeben:

```
aws sesv2 list-custom-verification-email-templates
```

Bearbeiten einer benutzerdefinierten Vorlage zur E-Mail-Verifizierung

Sie können eine benutzerdefinierte Verifizierungs-E-Mail-Vorlage unter Verwendung der `UpdateCustomVerificationEmailTemplate`-Operation bearbeiten. Diese Operation akzeptiert die gleichen Eingaben wie die `CreateCustomVerificationEmailTemplate`-Operation (d. h. die `TemplateName`, `FromEmailAddress`, `TemplateSubject`, `TemplateContent`, `SuccessRedirectionURL` und `FailureRedirectionURL`-Attribute). Jedoch sind bei der `UpdateCustomVerificationEmailTemplate`-Operation keine dieser Attribute erforderlich. Wenn Sie einen Wert für `TemplateName` übergeben, der identisch mit dem einer vorhandenen benutzerdefinierten Verifizierungs-E-Mail-Vorlage ist, überschreiben die angegebenen Attribute diejenigen, die ursprünglich in der Vorlage waren.

Senden von Verifizierungs-E-Mails mit benutzerdefinierten Vorlagen

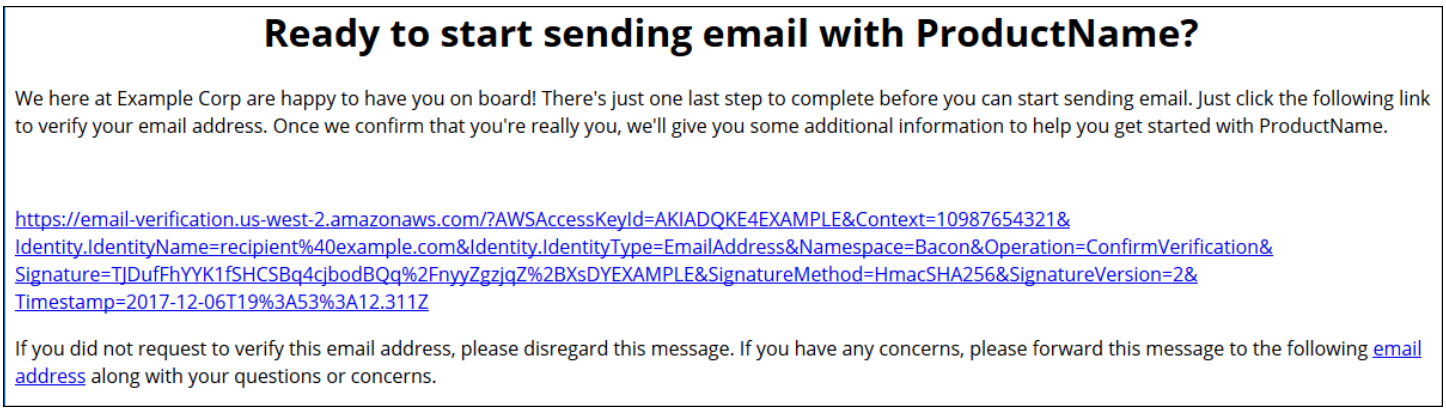
Nachdem Sie mindestens eine benutzerdefinierte E-Mail-Vorlage für die Bestätigung erstellt haben, können Sie diese an Ihre Kunden senden, indem Sie den SendCustomVerificationEmailAPI-Vorgang aufrufen. Sie können den `SendCustomVerificationEmail` Vorgang aufrufen, indem Sie eine der Optionen AWS SDKs oder die verwenden AWS CLI. Die `SendCustomVerificationEmail`-Operation akzeptiert die folgenden Eingaben:

Attribut	Description
`EmailAddress`	Die E-Mail-Adresse, die überprüft wird.

Attribut	Description
`TemplateName`	Der Name der benutzerdefinierten Verifizierungs-E-Mail-Vorlage, der an die E-Mail-Adresse gesendet wird, die überprüft wird.
`ConfigurationSetName`	(Optional) Der Name eines Konfigurationssatzes, der verwendet wird, wenn die Verifizierungs-E-Mail gesendet wird.

Angenommen, Ihre Kunden registrieren sich für Ihren Service mit einem Formular in Ihrer Anwendung. Wenn der Kunde das Formular ausfüllt und absendet, ruft Ihre Anwendung die `SendCustomVerificationEmail`-Operation auf, wodurch die E-Mail-Adresse des Kunden und der Name der Vorlage, die Sie verwenden möchten, weitergeleitet werden.

Der Kunde erhält eine E-Mail, welche die angepasste E-Mail-Vorlage verwendet, die Sie erstellt haben. Amazon SES fügt dem Empfänger automatisch einen eindeutigen Link sowie eine kurze Erläuterung hinzu. Die folgende Abbildung zeigt ein Beispiel für eine Verifizierungs-E-Mail, welche die in Erstellen einer benutzerdefinierten Vorlage zur E-Mail-Verifizierung erstellte Vorlage verwendet.



Ready to start sending email with ProductName?

We here at Example Corp are happy to have you on board! There's just one last step to complete before you can start sending email. Just click the following link to verify your email address. Once we confirm that you're really you, we'll give you some additional information to help you get started with ProductName.

https://email-verification.us-west-2.amazonaws.com/?AWSAccessKeyId=AKIADQKE4EXAMPLE&Context=10987654321&Identity.IdentityName=recipient%40example.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=TJDufFhYYK1fSHCSBq4cjbodBQq%2FnyyZgzjqZ%2BXsDYEXAMPLE&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2017-12-06T19%3A53%3A12.311Z

If you did not request to verify this email address, please disregard this message. If you have any concerns, please forward this message to the following email address along with your questions or concerns.

Benutzerdefinierte Verifizierungs-E-Mail – Häufig gestellte Fragen

Dieser Abschnitt enthält Antworten auf häufig gestellte Fragen zu der Funktion der benutzerdefinierten Verifizierungs-E-Mail-Vorlage.

F1. Wie viele benutzerdefinierte Verifizierungs-E-Mail-Vorlagen können erstellt werden?

Sie können bis zu 50 benutzerdefinierte Verifizierungs-E-Mail-Vorlagen pro Amazon SES-Konto erstellen.

F2. Wie werden benutzerdefinierte Verifizierungs-E-Mails dem Empfänger angezeigt?

Benutzerdefinierte Verifizierungs-E-Mails umfassen die Inhalte, die Sie beim Erstellen der Vorlage angegeben haben, gefolgt von einem Link, auf den die Empfänger klicken müssen, um ihre E-Mail-Adressen zu überprüfen.

F3. Kann ich eine Vorschau der benutzerdefinierten Verifizierungs-E-Mail sehen?

Wenn Sie eine Vorschau einer benutzerdefinierten Verifizierungs-E-Mail sehen möchten, verwenden Sie die `SendCustomVerificationEmail`-Operation, um eine Verifizierungs-E-Mail an eine Adresse zu senden, die Sie besitzen. Wenn Sie nicht auf den Verifizierungs-Link klicken, erstellt Amazon SES keine neue Identität. Wenn Sie auf den Verifizierungs-Link klicken, können Sie optional die neu erstellte Identität mithilfe der `DeleteIdentity`-Operation löschen.

F4. Kann ich meinen benutzerdefinierten Verifizierungs-E-Mail-Vorlagen Abbilder hinzufügen?

Sie können Abbilder für Ihre Vorlagen mithilfe der Base64-Kodierung in den HTML-Code einbetten. Wenn Sie Abbilder auf diese Weise einbetten, wandelt Amazon SES diese automatische in Anlagen um. Sie können ein Abbild in der Befehlszeile codieren, indem Sie einen der folgenden Befehle ausgeben:

Linux, macOS, or Unix

```
base64 -i imagefile.png | tr -d '\n' > output.txt
```

Windows

```
certutil -encodehex -f imagefile.png output.txt 0x40000001
```

Ersetzen Sie *`imagefile.png`* durch den Namen der Datei, die Sie kodieren möchten. In den beiden Befehlen oben wird das Base64-kodierte Abbild in gespeichert `output.txt`.

Sie können das Base64-kodierte Abbild einbetten, indem Sie Folgendes in den HTML-Code für die Vorlage einschließen: `<img src="`*`base64EncodedImage`*`"/>`

Im obigen Beispiel ersetzen Sie *`png`* mit dem Dateityp des kodierten Abbilds (z. B. JPG oder GIF) und ersetzen *`base64EncodedImage`* mit dem Base64-kodierten Abbild (d. h., den Inhalt `output.txt` von einem der oben genannten Befehle).

F5. Gibt es Beschränkungen für die Inhalte, die in benutzerdefinierten Verifizierungs-E-Mail-Vorlagen enthalten sein können?

Benutzerdefinierte Verifizierungs-E-Mail-Vorlagen dürfen eine Größe von 10 MB nicht überschreiten. Darüber hinaus können benutzerdefinierte Verifizierungs-E-Mail-Vorlagen, die HTML-Code enthalten, ausschließlich die Tags und Attribute verwenden, die in der folgenden Tabelle aufgelistet sind:

HTML-Tag	Zulässige Attribute
abbr	class, id, style, title
acronym	class, id, style, title
address	class, id, style, title
area	class, id, style, title
b	class, id, style, title
bdo	class, id, style, title
big	class, id, style, title
blockquote	cite, class, id, style, title
body	class, id, style, title
br	class, id, style, title
button	class, id, style, title
caption	class, id, style, title
center	class, id, style, title
cite	class, id, style, title
code	class, id, style, title
col	class, id, span, style, title, width

HTML-Tag	Zulässige Attribute
colgroup	class, id, span, style, title, width
dd	class, id, style, title
del	class, id, style, title
dfn	class, id, style, title
dir	class, id, style, title
div	class, id, style, title
dl	class, id, style, title
dt	class, id, style, title
em	class, id, style, title
fieldset	class, id, style, title
font	class, id, style, title
form	class, id, style, title
h1	class, id, style, title
h2	class, id, style, title
h3	class, id, style, title
h4	class, id, style, title
h5	class, id, style, title
h6	class, id, style, title
head	class, id, style, title
hr	class, id, style, title

HTML-Tag	Zulässige Attribute
html	class, id, style, title
i	class, id, style, title
img	align, alt, class, height, id, src, style, title, width
input	class, id, style, title
ins	class, id, style, title
kbd	class, id, style, title
label	class, id, style, title
legend	class, id, style, title
li	class, id, style, title
map	class, id, style, title
menu	class, id, style, title
ol	class, id, start, style, title, type
optgroup	class, id, style, title
option	class, id, style, title
p	class, id, style, title
pre	class, id, style, title
q	cite, class, id, style, title
s	class, id, style, title
samp	class, id, style, title

HTML-Tag	Zulässige Attribute
select	class, id, style, title
small	class, id, style, title
span	class, id, style, title
strike	class, id, style, title
strong	class, id, style, title
sub	class, id, style, title
sup	class, id, style, title
table	class, id, style, summary, title, width
tbody	class, id, style, title
td	abbr, axis, class, colspan, id, rowspan, style, title, width
textarea	class, id, style, title
tfoot	class, id, style, title
th	abbr, axis, class, colspan, id, rowspan, scope, style, title, width
thead	class, id, style, title
tr	class, id, style, title
tt	class, id, style, title
u	class, id, style, title
ul	class, id, style, title, type

HTML-Tag	Zulässige Attribute
`var`	`class, id, style, title`

> **Note**
>
> Benutzerdefinierte Verifizierungs-E-Mail-Vorlagen können keine Kommentar-Tags enthalten.

F6. Wie viele bestätigte E-Mail-Adressen können in meinem Konto vorhanden sein?

Ihr Amazon SES SES-Konto kann bis zu 10.000 verifizierte Identitäten in jeder AWS Region haben. In Amazon SES schließen Identitäten sowohl bestätigte Domänen als auch E-Mail-Adressen mit ein.

F7. Kann ich benutzerdefinierte Verifizierungs-E-Mail-Vorlagen unter Verwendung der Amazon SES-Konsole erstellen?

Derzeit können benutzerdefinierte Verifizierungs-E-Mails nur mit der Amazon SES-API erstellt, bearbeitet oder gelöscht werden.

F8. Kann ich Öffnungs- und Klickereignisse verfolgen, die auftreten, wenn Kunden benutzerdefinierte Verifizierungs-E-Mails erhalten?

Benutzerdefinierte Verifizierungs-E-Mails können keine Öffnungs- oder Klickverfolgung enthalten.

F9. Können benutzerdefinierte Verifizierungs-E-Mails benutzerdefinierte Header enthalten?

Benutzerdefinierte Verifizierungs-E-Mails können keine benutzerdefinierten Header enthalten.

F10. Kann ich den Text entfernen, der in benutzerdefinierten Verifizierungs-E-Mails unten angezeigt wird?

Der folgende Text wird automatisch an das Ende jeder benutzerdefinierten Verifizierungs-E-Mail hinzugefügt und kann nicht entfernt werden:

Wenn Sie die Verifizierung dieser E-Mail-Adresse nicht angefordert haben, ignorieren Sie diese Nachricht.

F11. Sind benutzerdefinierte Verifizierungs-E-Mails mit DKIM signiert?

Damit Verifizierungs-E-Mails mit DKIM signiert werden, muss die E-Mail-Adresse, die Sie beim Erstellen der Verifizierungs-E-Mail-Vorlage im `FromEmailAddress`-Attribut angeben, so konfiguriert werden, dass eine DKIM-Signatur erstellt wird. Weitere Informationen zur Einrichtung von DKIM für Domänen und E-Mail-Adressen finden Sie unter the section called “Authentifizierung Ihrer E-Mails mit DKIM”.

F12. Warum werden die API-Operationen für die benutzerdefinierte Verifizierungs-E-Mail-Vorlage nicht im SDK oder in der CLI angezeigt?

Wenn Sie die benutzerdefinierten E-Mail-Vorlagenoperationen für die Bestätigung nicht in einem SDK oder dem verwenden können AWS CLI, verwenden Sie möglicherweise eine ältere Version des SDK oder der CLI. Die Funktionen für benutzerdefinierte E-Mail-Vorlagen zur Bestätigung sind in den folgenden Versionen verfügbar SDKs und CLIs:

- Version 1.14.6 oder höher von AWS Command Line Interface
- Version 3.3.205.0 oder höher von AWS SDK für .NET
- Version 1.3.20170531.19 oder höher des SDK for C++ AWS
- Version 1.12.43 oder höher von AWS SDK für Go
- Version 1.11.245 oder höher von AWS SDK für Java
- Version 2.166.0 oder höher von AWS SDK für JavaScript
- Version 3.45.2 oder höher von AWS SDK für PHP
- Version 1.5.1 oder höher von AWS SDK für Python (Boto)
- `aws-sdk-ses`-Gem in AWS SDK für Ruby, Version 1.5.0 oder höher

F13. Warum erhalte ich **`ProductionAccessNotGranted`**-Fehler, wenn ich benutzerdefinierte Verifizierungs-E-Mails sende?

Der `ProductionAccessNotGranted`-Fehler zeigt an, dass sich Ihr Konto noch in der Amazon SES-Sandbox befindet. Sie können benutzerdefinierte Verifizierungs-E-Mails nur senden, wenn Ihr Konto aus der Sandbox entfernt wurde. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).

Verifizieren von Identitäten in Amazon SES

In der Amazon SES SES-Konsole können Sie Ihre erstellten Identitäten für jede Identität anzeigen AWS-Region, eine Identität öffnen, um ihre Detaileinstellungen zu sehen und zu bearbeiten, einen Standardkonfigurationssatz zuordnen oder eine oder mehrere Identitäten löschen.

> **Note**
>
> Die in diesem Abschnitt genannten Verfahren gelten nur für Identitäten in den ausgewählten. AWS-Region Um Identitäten zu verwalten, die in mehr als einer Region erstellt wurden, wiederholen Sie die Verfahren für jede Region. AWS-Region

Inhalt

- Identitäten mit der SES-Konsole anzeigen
- Löschen Sie eine Identität mit der SES-Konsole
- Bearbeiten Sie eine Identität mit der SES-Konsole
- Bearbeiten Sie eine Identität, um einen Standardkonfigurationssatz mithilfe der SES-API zu verwenden
- Rufen Sie den von der Identität verwendeten Standardkonfigurationssatz mithilfe der SES-API ab
- Überschreiben Sie den aktuellen Standardkonfigurationssatz, der von der Identität verwendet wird, mithilfe der SES-API

Identitäten mit der SES-Konsole anzeigen

Sie können die Amazon SES SES-Konsole verwenden, um Domänen- und E-Mail-Adressidentitäten anzuzeigen, die verifiziert wurden oder deren Überprüfung noch aussteht. Sie können auch die Identitäten anzeigen, für die die Überprüfung nicht erfolgreich war.

So zeigen Sie Ihre Domain- und E-Mail-Adressidentitäten an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie in der Konsole mithilfe der Regionsauswahl die Region aus, AWS-Region für die Sie Ihre Identitätsliste anzeigen möchten.

> **Note**
>
> Diese Prozedur zeigt nur eine Liste mit Identitäten für die ausgewählte AWS-Region aus.

3. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus. In der Tabelle Loaded identities (Geladene Identitäten) werden die Domänen- und E-Mail-Adressidentitäten angezeigt. Die Spalte Status wird angezeigt, ob eine Identität überprüft wurde, eine Überprüfung aussteht oder der Überprüfungsprozess fehlgeschlagen ist - Definitionen aller möglichen Statuswerte lauten wie folgt:

   - Bestätigt – Ihre Identität wurde erfolgreich für den Versand in SES überprüft.
   - Fehler – SES konnte Ihre Identität nicht überprüfen. Wenn es sich um eine Domäne handelt, bedeutet dies, dass SES die DNS-Datensätze nicht innerhalb von 72 Stunden erkennen konnte. Wenn es sich um eine E-Mail-Adresse handelt, bedeutet dies, dass die Bestätigungs-E-Mail, die an die E-Mail-Adresse gesendet wurde, nicht innerhalb von 24 Stunden bestätigt wurde.
   - Ausstehend – SES versucht immer noch, die Identität zu überprüfen.
   - Vorübergehender Fehler – Für eine zuvor überprüfte Domäne prüft SES regelmäßig nach dem für die Überprüfung erforderlichen DNS-Datensatz. Wenn SES den Datensatz irgendwann nicht erkennen kann, ändert sich der Status in Vorübergehender Fehler. SES prüft 72 Stunden lang erneut nach dem DNS-Datensatz, und wenn es den Datensatz nicht erkennen kann, ändert sich der Domänenstatus in Fehler. Wenn es in der Lage ist, den Datensatz zu erkennen, ändert sich der Domänenstatus in Bestätigt.
   - Nicht begonnen – Sie haben den Verifizierungsprozess noch nicht begonnen.
4. Um Identitäten nach Überprüfungsstatus zu sortieren, wählen Sie die Spalte Status.
5. Um die Detailseite einer Identität anzuzeigen, wählen Sie die Identität aus, die Sie anzeigen möchten.

Löschen Sie eine Identität mit der SES-Konsole

Sie können die Amazon SES SES-Konsole verwenden, um eine Domain- oder E-Mail-Adressidentität aus Ihrem Konto im ausgewählten Bereich zu entfernen AWS-Region.

So entfernen Sie eine Domänen- oder E-Mail-Adressidentität

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie in der Konsole mit der Regionsauswahl die AWS-Region aus, aus der Sie eine oder mehrere Identitäten löschen möchten.
3. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.

   In der Tabelle Loaded identities (Geladene Identitäten) wird eine Liste der Domänen- und E-Mail-Adressidentitäten angezeigt.
4. In der Spalte Identity (Identität) wählen Sie die Identität, die Sie löschen möchten. Sie können mehrere Identitäten löschen, indem Sie das Kontrollkästchen neben jeder Identität, die Sie löschen möchten.
5. Wählen Sie Löschen aus.

Bearbeiten Sie eine Identität mit der SES-Konsole

Sie können die Amazon SES SES-Konsole verwenden, um die Identität einer Domain oder E-Mail-Adresse in Ihrem Konto im ausgewählten Bereich zu bearbeiten AWS-Region.

Um die Identität einer Domain oder E-Mail-Adresse zu bearbeiten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie in der Konsole mit der Regionsauswahl die AWS-Region aus, von der Sie eine oder mehrere Identitäten bearbeiten möchten.
3. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.

   In der Tabelle Loaded identities (Geladene Identitäten) wird eine Liste der Domänen- und E-Mail-Adressidentitäten angezeigt.
4. Wählen Sie in Identity (Identität) die Identität aus, die Sie bearbeiten möchten (indem Sie direkt auf den Identitätsnamen klicken, anstatt das Kontrollkästchen zu aktivieren).
5. Wählen Sie auf der Detailseite der Identität die Registerkarte mit den Kategorien aus, die Sie bearbeiten möchten.

6. Wählen Sie in einem der kategorialen Container der ausgewählten Registerkarte die Schaltfläche Edit (Bearbeiten) des Attributs, das Sie bearbeiten möchten, nehmen Sie Ihre Änderungen vor und wählen Sie dann Save changes (Änderungen speichern).

   a. Wenn Sie Attribute auf der Registerkarte Authentifizierung bearbeiten möchten und Ihre Domain-Identität in Amazon Route 53 gehostet wird und Sie deren DNS-Einträge noch nicht veröffentlicht haben, wird in einem oder beiden der DomainKeys Identified Mail (DKIM) - oder Custom MAIL FROM Domain-Container die Schaltfläche DNS-Einträge auf Route53 veröffentlichen (neben der Schaltfläche Bearbeiten) angezeigt.

      > **Note**
      >
      > Die Registerkarte Authentication (Authentifizierung) ist nur vorhanden, wenn Ihr Konto über eine verifizierte Domäne oder eine E-Mail-Adresse verfügt, die eine verifizierte Domäne in Ihrem Konto verwendet.

   b. Sie können die DNS-Datensätze direkt über die Schaltfläche Publish DNS records to Route 53 (DNS-Einträge auf Route53 veröffentlichen) veröffentlichen – klicken Sie einfach darauf, ein Bestätigungsbanner wird angezeigt und die Schaltfläche Publish DNS records to Route53 (DNS-Datensätze auf Route53 veröffentlichen) ist für den jeweiligen Container nicht mehr sichtbar.

7. Wiederholen Sie die Schritte 5 und 6 für jedes Attribut der Identität, die Sie bearbeiten möchten.

Bearbeiten Sie eine Identität, um einen Standardkonfigurationssatz mithilfe der SES-API zu verwenden

Sie können den PutEmailIdentityConfigurationSetAttributesVorgang verwenden, um einer vorhandenen E-Mail-Identität einen Standardkonfigurationssatz hinzuzufügen oder daraus zu entfernen.

> **Note**
>
> Bevor Sie die Verfahren in diesem Abschnitt abschließen, müssen Sie zunächst die AWS CLI installieren und konfigurieren. Weitere Informationen finden Sie im AWS Command Line Interface -Benutzerhandbuch.

Um einen Standardkonfigurationssatz hinzuzufügen, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile den folgenden Befehl ein, um den PutEmailIdentityConfigurationSetAttributesVorgang zu verwenden.

```
aws sesv2 put-email-identity-configuration-set-attributes --email-identity ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Ersetzen Sie es in den vorherigen Befehlen *ADDRESS-OR-DOMAIN* durch die E-Mail-Identität, die Sie überprüfen möchten. *CONFIG-SET*Ersetzen Sie es durch den Namen des Konfigurationssatzes, den Sie als Standardkonfigurationssatz für die Identität festlegen möchten.

Bei erfolgreicher Ausführung wird der Befehl ohne Ausgabe beendet.

Um einen Standardkonfigurationssatz zu entfernen, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile den folgenden Befehl ein, um den PutEmailIdentityConfigurationSetAttributesVorgang zu verwenden.

```
aws sesv2 put-email-identity-configuration-set-attributes --email-identity ADDRESS-OR-DOMAIN
```

Ersetzen Sie es in den vorherigen Befehlen *ADDRESS-OR-DOMAIN* durch die E-Mail-Identität, die Sie überprüfen möchten.

Bei erfolgreicher Ausführung wird der Befehl ohne Ausgabe beendet.

Rufen Sie den von der Identität verwendeten Standardkonfigurationssatz mithilfe der SES-API ab

Sie können den GetEmailIdentityVorgang verwenden, um gegebenenfalls den Standardkonfigurationssatz für eine E-Mail-Identität zurückzugeben.

> **Note**
>
> Bevor Sie die Verfahren in diesem Abschnitt abschließen, müssen Sie zunächst die AWS CLI installieren und konfigurieren. Weitere Informationen finden Sie im AWS Command Line Interface -Benutzerhandbuch.

Um einen Standardkonfigurationssatz zurückzugeben, verwenden Sie den AWS CLI

- Geben Sie in der Befehlszeile den folgenden Befehl ein, um die GetEmailIdentityOperation zu verwenden.

```
aws sesv2 get-email-identity --email-identity ADDRESS-OR-DOMAIN
```

Ersetzen Sie die Befehle in den vorherigen Befehlen *ADDRESS-OR-DOMAIN* durch die E-Mail-Identität, für die Sie den Standardkonfigurationssatz, falls vorhanden, wissen möchten.

Bei erfolgreicher Ausführung wird ein JSON-Objekt mit den Details der E-Mail-Identität bereitgestellt.

Überschreiben Sie den aktuellen Standardkonfigurationssatz, der von der Identität verwendet wird, mithilfe der SES-API

Sie können den SendEmailVorgang verwenden, um E-Mails mit einem anderen Konfigurationssatz zu senden. Dadurch wird der Standardkonfigurationssatz der Identität durch den von Ihnen angegebenen Konfigurationssatz außer Kraft gesetzt.

> **Note**
>
> Bevor Sie die Verfahren in diesem Abschnitt abschließen, müssen Sie zunächst die AWS CLI installieren und konfigurieren. Weitere Informationen finden Sie im AWS Command Line Interface -Benutzerhandbuch.

Um einen Standardkonfigurationssatz mit dem zu überschreiben AWS CLI

- Geben Sie in der Befehlszeile den folgenden Befehl ein, um den SendEmailVorgang zu verwenden.

```
aws sesv2 send-email --destination file://DESTINATION-JSON --content file://CONTENT-JSON --from-email-address ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

*DESTINATION-JSON*Ersetzen Sie in den vorherigen Befehlen durch Ihre JSON-Zieldatei, *CONTENT-JSON* durch Ihre JSON-Inhaltsdatei, *ADDRESS-OR-DOMAIN* durch Ihre FROM-E-Mail-

Adresse und *CONFIG-SET* durch den Namen des Konfigurationssatzes, den Sie anstelle des Standardkonfigurationssatzes für die Identität verwenden möchten.

Wenn der Befehl erfolgreich ausgeführt wird, gibt er eine `MessageId` aus.

Konfigurieren von Identitäten in Amazon SES

Amazon Simple Email Service (Amazon SES) nutzt zum Senden von E-Mail das SMTP (Simple Mail Transfer Protocol). Da SMTP selbst keine Authentifizierung bereitstellt, kann ein Spammer E-Mails versenden, die augenscheinlich von jemand anderem stammen, während der tatsächliche Ursprung verborgen bleibt. Durch die Fälschung von E-Mail-Headern und das Spoofing von Quell-IP-Adressen können Spammer Empfängern vortäuschen, dass die E-Mail-Nachrichten, die sie erhalten, echt sind.

Die meisten ISPs Unternehmen, die E-Mail-Verkehr weiterleiten, ergreifen Maßnahmen, um zu bewerten, ob E-Mails legitim sind. Eine dieser ISPs Maßnahmen besteht darin, festzustellen, ob eine E-Mail authentifiziert ist. Für die Authentifizierung ist es erforderlich, dass Sender verifizieren, dass sie der Besitzer des sendenden Kontos sind. ISPs Weigern Sie sich in einigen Fällen, E-Mails weiterzuleiten, die nicht authentifiziert sind. Für optimale Zustellbarkeit empfehlen wir, dass Sie Ihre E-Mails authentifizieren.

In den folgenden Abschnitten werden die beiden ISPs verwendeten Authentifizierungsmechanismen — Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) — beschrieben. Außerdem finden Sie Anweisungen zur Verwendung dieser Standards mit Amazon SES.

- Weitere Informationen zu SPF, welches eine Möglichkeit bietet, eine E-Mail-Nachricht zurück zu dem System zu verfolgen, von dem sie gesendet wurde, finden Sie unter Authentifizierung Ihrer E-Mails mit SPF in Amazon SES.
- Weitere Informationen über DKIM, einen Standard, mit dem Sie Ihre E-Mail-Nachrichten signieren können, um nachzuweisen ISPs , dass Ihre Nachrichten legitim sind und während der Übertragung nicht verändert wurden, finden Sie unter. Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES
- Weitere Informationen dazu, wie Sie Domain-based Message Authentication, Reporting and Conformance (DMARC) einhalten, was sich auf SPF und DKIM stützt, finden Sie unter Einhaltung des DMARC-Authentifizierungsprotokolls in Amazon SES.

E-Mail-Authentifizierungsmethoden

Amazon Simple Email Service (Amazon SES) nutzt zum Senden von E-Mail das SMTP (Simple Mail Transfer Protocol). Da SMTP selbst keine Authentifizierung bereitstellt, kann ein Spammer E-Mails

versenden, die augenscheinlich von jemand anderem stammen, während der tatsächliche Ursprung verborgen bleibt. Durch die Fälschung von E-Mail-Headern und das Spoofing von Quell-IP-Adressen können Spammer Empfängern vortäuschen, dass die E-Mail-Nachrichten, die sie erhalten, echt sind.

Die meisten ISPs Unternehmen, die E-Mail-Verkehr weiterleiten, ergreifen Maßnahmen, um zu bewerten, ob E-Mails legitim sind. Eine dieser ISPs Maßnahmen besteht darin, festzustellen, ob eine E-Mail authentifiziert ist. Für die Authentifizierung ist es erforderlich, dass Sender verifizieren, dass sie der Besitzer des sendenden Kontos sind. ISPs Weigern Sie sich in einigen Fällen, E-Mails weiterzuleiten, die nicht authentifiziert sind. Für optimale Zustellbarkeit empfehlen wir, dass Sie Ihre E-Mails authentifizieren.

Inhalt

- Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES
- Authentifizierung Ihrer E-Mails mit SPF in Amazon SES
- Verwenden einer benutzerdefinierten MAIL FROM-Domäne
- Einhaltung des DMARC-Authentifizierungsprotokolls in Amazon SES
- Verwenden von BIMI in Amazon SES

Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES

DomainKeys Identified Mail (DKIM) ist ein E-Mail-Sicherheitsstandard, der sicherstellen soll, dass eine E-Mail, die behauptet, von einer bestimmten Domain zu stammen, tatsächlich vom Inhaber dieser Domain autorisiert wurde. Es verwendet Kryptografie für öffentliche Schlüssel, um eine E-Mail mit einem privaten Schlüssel zu signieren. Empfängerserver können dann einen öffentlichen Schlüssel verwenden, der im DNS einer Domäne veröffentlicht wurde, um zu überprüfen, ob Teile der E-Mail während des Transports nicht geändert wurden.

DKIM-Signaturen sind optional. Sie können Ihre E-Mail mit einer DKIM-Signatur signieren, um die Zustellbarkeit mit DKIM-konformen E-Mail-Anbietern zu verbessern. Amazon SES bietet zwei Möglichkeiten zum Signieren von Nachrichten mit einer DKIM-Signatur:

- Easy DKIM: SES generiert ein öffentlich-privates Schlüsselpaar und fügt automatisch eine DKIM-Signatur zu allen Nachrichten hinzu, die Sie über diese Identität versenden, vgl. Easy DKIM in Amazon SES.
- Deterministic Easy DKIM (DEED): Ermöglicht es Ihnen, eine konsistente DKIM-Signatur über mehrere Kanäle hinweg aufrechtzuerhalten, AWS-Regionen indem Sie Replikatidentitäten

erstellen, die automatisch die DKIM-Signaturattribute als übergeordnete Identität erben, wenn Easy DKIM verwendet wird, siehe. Verwenden von Deterministic Easy DKIM (DEED) in Amazon SES

- BYODKIM (Bring Your Own DKIM): Sie stellen Ihr eigenes öffentlich-privates Schlüsselpaar bereit, und SES fügt eine DKIM-Signatur zu allen E-Mail-Nachrichten hinzu, die Sie über diese Identität versenden, vgl. Bereitstellen Ihres eigenen DKIM-Authentifizierungs-Tokens (BYODKIM) in Amazon SES.
- DKIM-Signatur manuell hinzufügen: Sie fügen ihre eigene DKIM-Signatur jeder E-Mail-Nachricht hinzu, die Sie mit der `SendRawEmail`-API senden, vgl. Manuelle DKIM-Signierung in Amazon SES.

Länge des DKIM-Schlüssellänge

Da viele DNS-Anbieter jetzt die DKIM 2048-Bit-RSA-Verschlüsselung vollständig unterstützen, unterstützt Amazon SES auch DKIM 2048, um eine sicherere Authentifizierung von E-Mails zu ermöglichen und verwendet sie daher als Standardschlüssellänge, wenn Sie Easy DKIM entweder über die API oder die Konsole konfigurieren. 2048-Bit-Schlüssel können in Bring Auch Ihr eigenes DKIM (BYODKIM), wobei Ihre Signaturschlüssellänge mindestens 1024 Bit und nicht mehr als 2048 Bit betragen muss.

Aus Gründen der Sicherheit und der Zustellbarkeit Ihrer E-Mails haben Sie bei der Konfiguration mit Easy DKIM die Wahl, entweder die Schlüssellängen von 1024 und 2048 Bit sowie die Flexibilität des Rückkehrs auf 1024 zu verwenden, falls Probleme auftreten, die von DNS-Anbietern verursacht werden, die 2048 immer noch nicht unterstützen. Wenn Sie eine neue Identität erstellen, wird diese standardmäßig mit DKIM 2048 erstellt, es sei denn, Sie geben 1024 an.

Um die Zustellbarkeit von Transit-E-Mails beizubehalten, gibt es Einschränkungen hinsichtlich der Häufigkeit, mit der Sie die DKIM-Schlüssellänge ändern können. Zu den Einschränkungen zählen:

- Es ist nicht möglich, auf die gleiche Schlüssellänge zu wechseln, die bereits konfiguriert ist.
- Es ist nicht möglich, mehr als einmal in einem Zeitraum von 24 Stunden auf eine andere Schlüssellänge zu wechseln (es sei denn, es handelt sich um das erste Downgrade auf 1024 in diesem Zeitraum).

Wenn Ihre E-Mail unterwegs ist, verwendet DNS Ihren öffentlichen Schlüssel, um Ihre E-Mail zu authentifizieren. Wenn Sie also Schlüssel zu schnell oder häufig ändern, kann DNS möglicherweise nicht in der Lage sein, Ihre E-Mail DKIM zu authentifizieren, da der frühere Schlüssel möglicherweise bereits ungültig ist, daher schützen diese Einschränkungen davor.

DKIM-Überlegungen

Wenn Sie Ihre E-Mails mit DKIM authentifizieren, gelten die folgenden Regeln:

- Sie müssen DKIM nur für die Domäne einrichten, die Sie bei Ihrer Absenderadresse verwenden. Sie müssen DKIM nicht für Domänen einrichten, die Sie bei der "Return-Path"-Adresse oder der Antwortadresse verwenden.
- Amazon SES ist in mehreren AWS Regionen verfügbar. Wenn Sie mehr als eine AWS -Region für den Versand von E-Mails verwenden, müssen Sie die DKIM-Einrichtung in jeder dieser Regionen durchführen, um sicherzustellen, dass all Ihre E-Mails mit einer DKIM-Signatur versehen werden.
- Da DKIM-Eigenschaften von der übergeordneten Domäne vererbt werden, gilt, wenn Sie eine Domäne mit DKIM-Authentifizierung überprüfen:
  - Die DKIM-Authentifizierung auch für alle Sub-Domäne dieser Domäne.
    - DKIM-Einstellungen für eine Sub-Domäne können die Einstellungen für die übergeordnete Domäne außer Kraft setzen, indem Sie die Vererbung deaktivieren, wenn Sie nicht möchten, dass die Sub-Domäne die DKIM-Authentifizierung verwendet. Sie kann später wieder aktiviert werden.
  - Die DKIM-Authentifizierung gilt auch für alle E-Mails, die von einer E-Mail-Identität gesendet werden, die in ihrer Adresse auf die DKIM-verifizierte Domäne verweist.
    - DKIM-Einstellungen für eine E-Mail-Adresse können die Einstellungen für die Sub-Domäne (sofern zutreffend) und die übergeordnete Domäne außer Kraft setzen, indem Sie die Vererbung deaktivieren, wenn Sie E-Mails ohne DKIM-Authentifizierung senden möchten. Sie kann später wieder aktiviert werden.

Verstehen geerbter DKIM-Signatureigenschaften

Es ist wichtig, zuerst zu verstehen, dass eine E-Mail-Adressenidentität ihre DKIM-Signatureigenschaften von ihrer übergeordneten Domäne erbt, wenn diese Domäne mit DKIM konfiguriert wurde, unabhängig davon, ob Easy DKIM oder BYODKIM verwendet wurde. Daher ist das Deaktivieren oder Aktivieren der DKIM-Signatur für die E-Mail-Adressenidentität in Kraft, wodurch die DKIM-Signatureigenschaften der Domäne basierend auf diesen wichtigen Fakten außer Kraft gesetzt werden:

- Wenn Sie DKIM bereits für die Domäne eingerichtet haben, zu der eine E-Mail-Adresse gehört, müssen Sie die DKIM-Signierung nicht auch für die E-Mail-Adressenidentität aktivieren.

- Wenn Sie DKIM für eine Domäne einrichten, authentifiziert Amazon SES automatisch jede E-Mail von jeder Adresse in dieser Domäne über die geerbten DKIM-Eigenschaften der übergeordneten Domäne.
- DKIM-Einstellungen für eine bestimmte E-Mail-Adressenidentität überschreiben automatisch die Einstellungen der übergeordneten Domäne oder Unterdomäne (sofern zutreffend), zu der die Adresse gehört.

Da die DKIM-Signatureigenschaften der E-Mail-Adressenidentität von der übergeordneten Domäne geerbt werden, müssen Sie, wenn Sie diese Eigenschaften überschreiben möchten, die hierarchischen Regeln für das Überschreiben beachten, wie in der folgenden Tabelle beschrieben.

Die übergeordnete Domäne hat die DKIM-Signatur nicht aktiviert	Die übergeordnete Domäne hat die DKIM-Signatur aktiviert
Sie können die DKIM-Signatur für die E-Mail-Adressenidentität nicht aktivieren.	Sie können die DKIM-Signatur für die E-Mail-Adressenidentität deaktivieren.
	Sie können die DKIM-Signatur für die E-Mail-Adressenidentität erneut aktivieren.

Es wird im Allgemeinen nie empfohlen, Ihre DKIM-Signierung zu deaktivieren, da die Gefahr besteht, dass Ihre Senderreputation beeinträchtigt wird und es das Risiko erhöht, dass Ihre gesendeten E-Mails in Junk- oder Spam-Ordner wandern oder Ihre Domäne manipuliert wird.

Es besteht jedoch die Möglichkeit, die von der Domäne geerbten DKIM-Signatureigenschaften für eine E-Mail-Adressenidentität für einen bestimmten Anwendungsfall oder außerhalb der Geschäftsentscheidung außer Kraft zu setzen, dass Sie möglicherweise die DKIM-Signatur dauerhaft oder vorübergehend deaktivieren oder sie zu einem späteren Zeitpunkt wieder aktivieren müssen. Siehe the section called “Überschreiben der DKIM-Signatur an der E-Mail-Adresse”.

Easy DKIM in Amazon SES

Wenn Sie Easy DKIM für eine Domänenidentität einrichten, fügt Amazon SES automatisch einen 2048-Bit-DKIM-Schlüssel zu jeder E-Mail hinzu, die Sie über diese Identität versenden. Sie können Easy DKIM mit der Amazon-SES-Konsole oder mit der API konfigurieren.

> **Note**
>
> Zum Einrichten von Easy DKIM müssen Sie die DNS-Einstellungen für Ihre Domäne ändern. Wenn Sie Route 53 als DNS-Anbieter verwenden, kann Amazon SES automatisch die entsprechenden Datensätze für Sie erstellen. Wenn Sie einen anderen DNS-Anbieter verwenden, finden Sie in der Dokumentation Ihres Anbieters weitere Informationen dazu, wie Sie die DNS-Einstellungen für Ihre Domäne ändern.

> **Warning**
>
> Wenn Sie derzeit BYODKIM aktiviert haben und zu Easy DKIM wechseln, beachten Sie, dass Amazon SES BYODKIM nicht zum Signieren Ihrer E-Mails verwendet, während Easy DKIM eingerichtet wird und sich Ihr DKIM-Status in einem ausstehenden Zustand befindet. Zwischen dem Moment, in dem Sie den Anruf tätigen, um Easy DKIM (entweder über die API oder die Konsole) zu aktivieren, und dem Moment, in dem SES Ihre DNS-Konfiguration bestätigen kann, können Ihre E-Mails von SES ohne DKIM-Signatur gesendet werden. Daher wird empfohlen, einen Zwischenschritt zu verwenden, um von einer DKIM-Signaturmethode zur anderen zu migrieren (z. B. die Verwendung einer Subdomain Ihrer Domäne mit aktivierter BYODKIM und deren Löschung nach Ablauf der Easy DKIM-Überprüfung) oder diese Aktivität gegebenenfalls während der Ausfallzeit Ihrer Anwendung durchzuführen.

Einrichten von Easy DKIM für eine verifizierte Domänenidentität

Das Verfahren in diesem Abschnitt wird optimiert, um nur die Schritte anzuzeigen, die zum Konfigurieren von Easy DKIM für eine bereits erstellte Domänenidentität erforderlich sind. Wenn Sie noch keine Domänenidentität erstellt haben oder alle verfügbaren Optionen zum Anpassen Ihrer Domänenidentität anzeigen möchten, z. B. die Verwendung eines Standardkonfigurationssatzes, einer benutzerdefinierten „MAIL FROM“-Domäne und Tags, finden Sie weitere Informationen unter the section called “Erstellen einer Domänenidentität”.

Ein Teil der Erstellung einer Easy DKIM-Domänenidentität ist die Konfiguration der DKIM-basierten Verifizierung, bei der Sie entweder den Amazon SES S-Standard von 2048 Bit akzeptieren oder den Standardwert durch Auswahl von 1024 Bit übersteuern können. Siehe .the section called “Länge des DKIM-Schlüssellänge”, um mehr über die DKIM-Signierung von Schlüssellängen und deren Änderung zu erfahren.

So richten Sie Easy DKIM für eine Domäne ein

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie in der Liste der Identitäten eine Identität aus, in der Identity type (Identitätstyp) Domain (Domäne) ist.

   > **Note**
   >
   > Informationen zum Erstellen oder Überprüfen einer Domäne finden Sie unter Erstellen einer Domänenidentität aus.

4. Wählen Sie auf der Registerkarte Authentifizierung im Container DomainKeysIdentified Mail (DKIM) die Option Bearbeiten aus.
5. Im Container Advanced DKIM settings (Erweiterte DKIM-Einstellungen) wählen Sie die Schaltfläche Easy DKIM im Feld Identity type (Identitätstyp).
6. Im Feld DKIM signing key length (Länge des DKIM-Signierschlüssels), wählen Sie entweder RSA_2048_BIT oder RSA_1024_BIT aus.
7. Im Feld DKIM signatures (DKIM-Unterschriften) aktivieren Sie das Kontrollkästchen Enabled (Aktiviert).
8. Wählen Sie Änderungen speichern aus.
9. Nachdem Sie Ihre Domänenidentität mit Easy DKIM konfiguriert haben, müssen Sie den Verifizierungsprozess bei Ihrem DNS-Anbieter abschließen – fahren Sie mit the section called “Verifizieren einer Domänenidentität” fort und befolgen Sie die DNS-Authentifizierungsverfahren für Easy DKIM.

Ändern der Länge des einfachen DKIM-Signaturschlüssels für eine Identität

Das Verfahren in diesem Abschnitt zeigt, wie Sie die für den Signaturalgorithmus erforderlichen Easy DKIM-Bits einfach ändern können. Obwohl eine Signaturlänge von 2048 Bit für die verbesserte Sicherheit immer bevorzugt wird, kann es Situationen geben, in denen Sie die 1024-Bit-Länge verwenden müssen, z. B. einen DNS-Anbieter verwenden müssen, der nur DKIM 1024 unterstützt.

Um die Zustellbarkeit von Transit-E-Mails zu erhalten, gibt es Einschränkungen hinsichtlich der Häufigkeit, mit der Sie Ihre DKIM-Schlüssellänge ändern oder umkehren können.

Wenn Ihre E-Mail unterwegs ist, verwendet DNS Ihren öffentlichen Schlüssel, um Ihre E-Mail zu authentifizieren. Wenn Sie Schlüssel zu schnell oder häufig ändern, kann DNS möglicherweise nicht in der Lage sein, Ihre E-Mail DKIM zu authentifizieren, da der frühere Schlüssel möglicherweise bereits ungültig ist. Daher schützen die folgenden Einschränkungen davor:

- Sie können nicht zu derselben Schlüssellänge wechseln, die bereits konfiguriert ist.
- Sie können innerhalb von 24 Stunden nicht mehr als einmal zu einer anderen Schlüssellänge wechseln (es sei denn, es handelt sich um das erste Downgrade auf 1024 in diesem Zeitraum).

Wenn Sie die folgenden Verfahren verwenden, um Ihre Schlüssellänge zu ändern, gibt die Konsole ein Fehlerbanner zurück, das besagt, dass die von Ihnen angegebene Eingabe ist ungültig zusammen mit dem Grund, warum es ungültig war.

So ändern Sie die DKIM-Signaturschlüssellängen-Bits

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie Easy DKIM aktivieren möchten.
4. Wählen Sie auf der Registerkarte Authentifizierung im Container DomainKeysIdentified Mail (DKIM) die Option Bearbeiten aus.
5. Im Container Advanced DKIM settings (Erweiterte DKIM-Einstellungen) wählen Sie entweder RSA_2048_BIT oder RSA_1024_BIT im Feld DKIM signing key length (Länge des DKIM-Signierschlüssels) aus.
6. Wählen Sie Änderungen speichern aus.

Verwenden von Deterministic Easy DKIM (DEED) in Amazon SES

Deterministic Easy DKIM (DEED) bietet eine Lösung für die Verwaltung mehrerer DKIM-Konfigurationen. AWS-Regionen Durch die Vereinfachung der DNS-Verwaltung und die Sicherstellung einer konsistenten DKIM-Signatur hilft Ihnen DEED dabei, Ihre E-Mail-Versandvorgänge in mehreren Regionen zu rationalisieren und gleichzeitig robuste E-Mail-Authentifizierungspraktiken aufrechtzuerhalten.

Was ist Deterministic Easy DKIM (DEED)?

Deterministic Easy DKIM (DEED) ist eine Funktion, die konsistente DKIM-Token für alle generiert, die auf einer übergeordneten Domain AWS-Regionen basieren, die mit Easy DKIM konfiguriert ist. Auf diese Weise können Sie Identitäten auf verschiedene Arten replizieren AWS-Regionen , die automatisch dieselbe DKIM-Signaturkonfiguration erben und beibehalten wie eine übergeordnete Identität, die derzeit mit Easy DKIM konfiguriert ist. Mit DEED müssen Sie DNS-Einträge für die übergeordnete Identität nur einmal veröffentlichen, und Replikatidentitäten verwenden dieselben DNS-Einträge, um den Domainbesitz zu überprüfen und die DKIM-Signatur zu verwalten.

Durch die Vereinfachung der DNS-Verwaltung und die Sicherstellung einer konsistenten DKIM-Signatur hilft Ihnen DEED dabei, Ihre E-Mail-Versandvorgänge in mehreren Regionen zu optimieren und gleichzeitig die besten E-Mail-Authentifizierungspraktiken beizubehalten.

Terminologie, die verwendet wird, wenn über DEED gesprochen wird:

- Übergeordnete Identität — Eine mit Easy DKIM konfigurierte verifizierte Identität, die als Quelle für die DKIM-Konfiguration für eine Replikatidentität dient.
- Replikatidentität — Eine Kopie einer übergeordneten Identität, die dasselbe DNS-Setup und dieselbe DKIM-Signaturkonfiguration verwendet.
- Übergeordnete Region — Die Region AWS-Region , in der eine übergeordnete Identität eingerichtet wird.
- Replikatregion — Eine Region AWS-Region , in der eine Replikatidentität eingerichtet wird.
- DEED-Identität — Jede Identität, die entweder als übergeordnete Identität oder als Replikatidentität verwendet wird. (Wenn eine neue Identität erstellt wird, wird sie zunächst als reguläre Identität (keine DEED) behandelt. Sobald jedoch ein Replikat erstellt wurde, wird die Identität als DEED-Identität betrachtet.)

Zu den wichtigsten Vorteilen der Verwendung von DEED gehören:

- Vereinfachtes DNS-Management — Veröffentlichen Sie DNS-Einträge nur einmal für die übergeordnete Identität.
- Einfacherer Betrieb in mehreren Regionen — Vereinfachen Sie den Prozess der Ausweitung des E-Mail-Versands auf neue Regionen.
- Geringerer Verwaltungsaufwand — Verwalten Sie DKIM-Konfigurationen zentral von der übergeordneten Identität aus.

So funktioniert Deterministic Easy DKIM (DEED)

Wenn Sie eine Replikatidentität erstellen, repliziert Amazon SES automatisch den DKIM-Signaturschlüssel von der übergeordneten Identität auf die Replikatidentität. Alle nachfolgenden DKIM-Schlüsselrotationen oder Änderungen der Schlüssellänge, die an der übergeordneten Identität vorgenommen werden, werden automatisch auf alle Replikatidentitäten übertragen.

Der Prozess umfasst den folgenden Arbeitsablauf:

1. Erstellen Sie eine übergeordnete Identität in einem, AWS-Region der Easy DKIM verwendet.
2. Richten Sie die erforderlichen DNS-Einträge für die übergeordnete Identität ein.
3. Erstellen Sie Replikatidentitäten unter „Andere AWS-Regionen“ und geben Sie dabei den Domänennamen und die DKIM-Signaturregion der übergeordneten Identität an.
4. Amazon SES repliziert automatisch die DKIM-Konfiguration des übergeordneten Elements auf die Replikatidentitäten.

Wichtige Überlegungen:

- Sie können kein Replikat einer Identität erstellen, die bereits ein Replikat ist.
- Für die übergeordnete Identität muss Easy DKIM aktiviert sein. Sie können keine Replikate von BYODKIM oder manuell signierte Identitäten erstellen.
- Übergeordnete Identitäten können erst gelöscht werden, wenn alle Replikatidentitäten gelöscht wurden.

Einrichtung einer Replikatidentität mit DEED

In diesem Abschnitt finden Sie Beispiele, die Ihnen zeigen, wie Sie mithilfe von DEED eine Replikatidentität erstellen und überprüfen, sowie die erforderlichen Berechtigungen.

Themen

- Eine Replikatidentität erstellen
- Die Konfiguration der Replikatidentität wird überprüft
- Erforderliche Berechtigungen zur Verwendung von DEED

Eine Replikatidentität erstellen

So erstellen Sie eine Replikatidentität:

1. Öffnen Sie in AWS-Region dem Bereich, in dem Sie eine Replikatidentität erstellen möchten, die SES-Konsole unter. https://console.aws.amazon.com/ses/

   (In der SES-Konsole werden Replikatidentitäten als globale Identitäten bezeichnet.)
2. Wählen Sie im Navigationsbereich Identitäten aus.
3. Wählen Sie Create identity (Identität erstellen).
4. Wählen Sie unter Identitätstyp die Option Domäne aus und geben Sie den Domänennamen einer vorhandenen, mit Easy DKIM konfigurierten Identität ein, die Sie replizieren und als übergeordnete Identität verwenden möchten.
5. Erweitern Sie Erweiterte DKIM-Einstellungen und wählen Sie Deterministic Easy DKIM aus.
6. Wählen Sie im Dropdownmenü Übergeordnete Region eine übergeordnete Region aus, in der sich eine von Easy DKIM signierte Identität mit demselben Namen befindet, den Sie für Ihre globale (Replikat-) Identität eingegeben haben. (Ihre Replikatregion ist standardmäßig die Region, mit der Sie sich bei der SES-Konsole angemeldet haben.)
7. Stellen Sie sicher, dass DKIM-Signaturen aktiviert sind.
8. (Optional) Fügen Sie Ihrer Domain-Identität einen oder mehrere Tags hinzu.
9. Überprüfen Sie die Konfiguration und wählen Sie Create identity aus.

Verwenden von AWS CLI:

Um eine Replikatidentität auf der Grundlage einer mit Easy DKIM konfigurierten übergeordneten Identität zu erstellen, müssen Sie den Domänennamen des übergeordneten Elements, die Region, in der Sie die Replikatidentität erstellen möchten, und die DKIM-Signaturregion des übergeordneten Elements angeben, wie in diesem Beispiel gezeigt:

```
aws sesv2 create-email-identity --email-identity example.com --region us-west-2 --dkim-signing-attributes '{"DomainSigningAttributesOrigin": "AWS_SES_US_EAST_1"}'
```

Für das obige Beispiel gilt:

1. Ersetzen Sie es durch die *example.com* Identität der übergeordneten Domäne, die repliziert wird.
2. *us-west-2*Ersetzen Sie durch die Region, in der die Replikatdomänenidentität erstellt wird.
3. *AWS_SES_US_EAST_1*Ersetzen Sie es durch die DKIM-Signaturregion des übergeordneten Unternehmens, die dessen Easy DKIM-Signaturkonfiguration darstellt, die auf die Replikatidentität repliziert wird.

> **Note**
>
> Das `AWS_SES_` Präfix gibt an, dass DKIM mithilfe von Easy DKIM für die übergeordnete Identität konfiguriert wurde, und `US_EAST_1` ist der Ort, an dem es erstellt wurde. AWS-Region

Die Konfiguration der Replikatidentität wird überprüft

Nachdem Sie die Replikatidentität erstellt haben, können Sie anhand der DKIM-Signaturkonfiguration der übergeordneten Identität überprüfen, ob sie korrekt konfiguriert wurde.

So überprüfen Sie eine Replikatidentität:

1. Öffnen Sie in AWS-Region dem Bereich, in dem Sie die Replikatidentität erstellt haben, die SES-Konsole unter. https://console.aws.amazon.com/ses/
2. Wählen Sie im Navigationsbereich Identitäten aus und wählen Sie in der Tabelle Identitäten die Identität aus, die Sie verifizieren möchten.
3. Auf der Registerkarte Authentifizierung gibt das DKIM-Konfigurationsfeld den Status an, und das Feld Übergeordnete Region gibt die Region an, die für die DKIM-Signaturkonfiguration der Identität mithilfe von DEED verwendet wird.

Verwenden von: AWS CLI

Verwenden Sie den `get-email-identity` Befehl zur Angabe des Domainnamens und der Region des Replikats:

```
aws sesv2 get-email-identity --email-identity example.com --region us-west-2
```

Die Antwort enthält den Wert der übergeordneten Region in den `SigningAttributesOrigin` Parameter, der bedeutet, dass die Replikatidentität erfolgreich mit der DKIM-Signaturkonfiguration der übergeordneten Identität konfiguriert wurde:

```
{
  "DkimAttributes": {
    "SigningAttributesOrigin": "AWS_SES_US_EAST_1"
  }
```

```
}
```

Erforderliche Berechtigungen zur Verwendung von DEED

Um DEED verwenden zu können, benötigen Sie:

1. Standardberechtigungen für die Erstellung von E-Mail-Identitäten in der Replikatregion.
2. Berechtigung zur Replikation des DKIM-Signaturschlüssels aus der übergeordneten Region.

Beispiel für eine IAM-Richtlinie für die DKIM-Replikation

Die folgende Richtlinie ermöglicht die Replikation von DKIM-Signaturschlüsseln von einer übergeordneten Identität in bestimmte Replikatregionen:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDKIMReplication",
      "Effect": "Allow",
      "Action": "ses:ReplicateEmailIdentityDKIMSigningKey",
      "Resource": "arn:aws:ses:us-east-1:123456789124:identity/example.com",
      "Condition": {
        "ForAllValues:StringEquals": {
           "ses:ReplicaRegion": ["us-east-1", "us-east-1"]
        }
      }
    }
  ]
}
```

Best Practices

Die folgenden bewährten Methoden werden empfohlen:

- Planen Sie Ihre übergeordneten Regionen und Replikatregionen — Berücksichtigen Sie die von Ihnen gewählte übergeordnete Region, da sie als Informationsquelle für die in Replikatregionen verwendete DKIM-Konfiguration dient.

- Verwenden Sie konsistente IAM-Richtlinien — Stellen Sie sicher, dass Ihre IAM-Richtlinien die DKIM-Replikation in allen vorgesehenen Regionen ermöglichen.
- Übergeordnete Identitäten aktiv lassen — Denken Sie daran, dass Ihre Replikatidentitäten die DKIM-Signaturkonfiguration der übergeordneten Identität erben. Aufgrund dieser Abhängigkeit können Sie eine übergeordnete Identität erst löschen, wenn alle Replikatidentitäten gelöscht sind.

Fehlerbehebung

Wenn Sie Probleme mit DEED haben, sollten Sie Folgendes beachten:

- Fehler bei der Überprüfung — Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen für die DKIM-Replikation verfügen.
- Verzögerungen bei der Replikation — Warten Sie etwas, bis die Replikation abgeschlossen ist, insbesondere bei der Erstellung neuer Replikatidentitäten.
- DNS-Probleme — Stellen Sie sicher, dass die DNS-Einträge für die übergeordnete Identität korrekt eingerichtet und weitergegeben wurden.

Bereitstellen Ihres eigenen DKIM-Authentifizierungs-Tokens (BYODKIM) in Amazon SES

Anstatt Easy DKIM zu verwenden, können Sie alternativ auch die DKIM-Authentifizierung konfigurieren, indem Sie Ihr eigenes Schlüsselpaar aus öffentlichem und privatem Schlüssel verwenden. Dieser Prozess wird auch als Bring Your Own DKIM (Verwendung der eigenen DKIM) (BYODKIM) bezeichnet.

Mit BYODKIM können Sie einen einzelnen DNS-Eintrag verwenden, um die DKIM-Authentifizierung für Ihre Domänen zu konfigurieren. Mit Easy DKIM müssen Sie hingegen drei separate DNS-Einträge veröffentlichen. Darüber hinaus können Sie mit BYODKIM die DKIM-Schlüssel für Ihre Domänen beliebig oft rotieren.

Themen in diesem Abschnitt:

- Schritt 1: Erstellen des Schlüsselpaars
- Schritt 2: Hinzufügen des Selektors und öffentlichen Schlüssels zur Domänenkonfiguration Ihres DNS-Anbieters
- Schritt 3: Konfigurieren und Überprüfen einer Domäne zur Verwendung von BYODKIM

> **Warning**
>
> Wenn Sie derzeit Easy DKIM aktiviert haben und zu BYODKIM wechseln, beachten Sie, dass Amazon SES Easy DKIM nicht zum Signieren Ihrer E-Mails verwendet, während BYODKIM eingerichtet wird und sich Ihr DKIM-Status in einem ausstehenden Zustand befindet. Zwischen dem Moment, in dem Sie den Anruf tätigen, um BYODKIM (entweder über die API oder die Konsole) zu aktivieren, und dem Moment, in dem SES Ihre DNS-Konfiguration bestätigen kann, können Ihre E-Mails von SES ohne DKIM-Signatur gesendet werden. Daher wird empfohlen, einen Zwischenschritt zu verwenden, um von einer DKIM-Signaturmethode zur anderen zu migrieren (z. B. die Verwendung einer Subdomäne Ihrer Domäne mit aktiviertem Easy DKIM und deren Löschung nach Ablauf der BYODKIM-Überprüfung) oder diese Aktivität gegebenenfalls während der Ausfallzeit Ihrer Anwendung durchzuführen.

Schritt 1: Erstellen des Schlüsselpaars

Um die Funktion Bring Your Own DKIM verwenden zu können, müssen Sie zunächst ein RSA-Schlüsselpaar erstellen.

Der von Ihnen generierte private Schlüssel muss das Format PKCS #1 oder PKCS #8 aufweisen, mindestens 1024-Bit-RSA-Verschlüsselung und bis zu 2048-Bit verwenden und mit Base64-Codierung (PEM) codiert sein. Für weitere Informationen über die DKIM-Signierung von Schlüssellängen und deren Änderung siehe the section called “Länge des DKIM-Schlüssellänge”.

> **Note**
>
> Sie können Anwendungen und Tools von Drittanbietern verwenden, um RSA-Schlüsselpaare zu generieren, solange der private Schlüssel mit mindestens 1024-Bit-RSA-Verschlüsselung und bis zu 2048-Bit generiert wird und mit Base64-Codierung (PEM) codiert ist.

Im folgenden Verfahren verwendet der Beispielcode, der den Befehl `openssl genrsa` zum Erstellen des Schlüsselpaares nutzt, welcher in die meisten Linux-, macOS- oder Unix-Betriebssysteme integriert ist, automatisch Base64-Codierung (PEM).

So erstellen Sie das Schlüsselpaar über die Befehlszeile von Linux, macOS oder Unix

1. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den privaten Schlüssel zu generieren und *nnnn* ihn durch eine Bitlänge von mindestens 1024 und bis zu 2048 zu ersetzen:

   ```
   openssl genrsa -f4 -out private.key nnnn
   ```

2. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den öffentlichen Schlüssel zu generieren:

   ```
   openssl rsa -in private.key -outform PEM -pubout -out public.key
   ```

Schritt 2: Hinzufügen des Selektors und öffentlichen Schlüssels zur Domänenkonfiguration Ihres DNS-Anbieters

Nachdem Sie nun ein Schlüsselpaar erstellt haben, müssen Sie den öffentlichen Schlüssel als TXT-Datensatz zur DNS-Konfiguration für Ihre Domäne hinzufügen.

So fügen den öffentlichen Schlüssel zur DNS-Konfiguration für Ihre Domäne hinzu

1. Melden Sie sich bei der Managementkonsole für Ihren DNS- oder Hosting-Anbieter an.
2. Fügen Sie einen neuen Textdatensatz zur DNS-Konfiguration für Ihre Domäne hinzu. Der Datensatz sollte das folgende Format verwenden:

Name	Typ	Wert
selector. _Domänens chlüssel. *example.com*	TXT	p= *yourPublicKey*

   Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

   - *selector*Ersetzen Sie es durch einen eindeutigen Namen, der den Schlüssel identifiziert.

     > **Note**
     >
     > Einige wenige DNS-Anbieter lassen keine Unterstriche (_) in den Namen von Datensätzen zu. Der Unterstrich im DKIM-Datensatznamen ist jedoch erforderlich.

Wenn Ihr DNS-Anbieter keine Unterstriche im Datensatznamen zulässt, bitten Sie das Kundensupport-Team des Anbieters um Hilfe.

- Ersetze es *example.com* durch deine Domain.
- *yourPublicKey*Ersetzen Sie es durch den öffentlichen Schlüssel, den Sie zuvor erstellt haben, und fügen Sie das p= Präfix hinzu, wie in der Spalte Wert oben gezeigt.

> **Note**
>
> Wenn Sie Ihren öffentlichen Schlüssel an Ihren DNS-Anbieter veröffentlichen (ihm hinzufügen), muss er wie folgt formatiert sein:
>
> - Sie müssen die erste und letzte Zeile (`-----BEGIN PUBLIC KEY-----` bzw. `-----END PUBLIC KEY-----`) des generierten öffentlichen Schlüssels löschen. Darüber hinaus müssen Sie die Zeilenumbrüche im generierten öffentlichen Schlüssel entfernen. Der resultierende Wert ist eine Zeichenfolge ohne Leerzeichen oder Zeilenumbrüche.
> - Sie müssen das Präfix p=, wie in der Spalte Value (Wert) der oben stehenden Tabelle gezeigt, einschließen.

Verschiedene Anbieter nutzen unterschiedliche Verfahren zum Aktualisieren von DNS-Datensätzen. Die folgende Tabelle enthält Links zur Dokumentation für einige gängige DNS-Anbieter. Diese Liste ist nicht vollständig und stellt keine Empfehlung dar. Wenn Ihr DNS-Anbieter nicht aufgeführt ist, bedeutet dies nicht, dass Sie die Domäne nicht mit Amazon SES verwenden können.

DNS/Hosting-Anbieter	Link zur Dokumentation
Amazon Route 53	Weitere Informationen finden Sie unter Bearbeiten von Datensätzen im Entwickle rhandbuch für Amazon Route 53.
GoDaddy	Hinzufügen eines TXT-Datensatzes (externer Link)

DNS/Hosting-Anbieter	Link zur Dokumentation
DreamHost	Wie füge ich benutzerdefinierte DNS-Daten sätze hinzu? (externer Link)
Cloudflare	Verwalten von DNS-Datensätzen in CloudFlare (externer Link)
HostGator	DNS-Einträge mit HostGator /eNom (externer Link) verwalten
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC Einträge für meine Domain hinzu? (externer Link)
Names.co.uk	Ändern der DNS-Einstellungen Ihrer Domänen (externer Link)
Wix	Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto (externer Link)

Schritt 3: Konfigurieren und Überprüfen einer Domäne zur Verwendung von BYODKIM

Sie können BYODKIM sowohl für neue Domänen (d. h. Domänen, die Sie derzeit nicht zum Senden von E-Mails über Amazon SES verwenden) als auch für vorhandene Domänen (d. h. für Domänen, die Sie bereits für die Verwendung mit Amazon SES eingerichtet haben) einrichten, mithilfe der Konsole oder AWS CLI. Bevor Sie die AWS CLI Verfahren in diesem Abschnitt verwenden können, müssen Sie zuerst die installieren und konfigurieren AWS CLI. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch..

Option 1: Erstellen einer neuen Domänenidentität, die BYODKIM verwendet

Dieser Abschnitt enthält Verfahren zum Erstellen einer neuen Domänenidentität, die BYODKIM verwendet. Eine neue Domänenidentität ist eine Domäne, die Sie zuvor nicht zum Senden von E-Mails über Amazon SES eingerichtet haben.

Wenn Sie eine vorhandene Domäne für die Verwendung von BYODKIM konfigurieren möchten, führen Sie stattdessen das unter Option 2: Konfigurieren einer vorhandenen Domänenidentität beschriebene Verfahren aus.

So erstellen Sie mit BYODKIM eine Identität aus der Konsole

- Folgen Sie den Verfahren unter Erstellen einer Domänenidentität und für Schritt 8 die spezifischen Anweisungen von BYODKIM.

Um eine Identität mit BYODKIM aus dem zu erstellen AWS CLI

Verwenden Sie die Operation `CreateEmailIdentity` in der Amazon-SES-API, um eine neue Domäne einzurichten.

1. Fügen Sie folgenden Code in einen Texteditor ein:

```
{
    "EmailIdentity":"example.com",
    "DkimSigningAttributes":{
        "DomainSigningPrivateKey":"privateKey",
        "DomainSigningSelector":"selector"
    }
}
```

   Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

   - Ersetzen Sie *example.com* durch die Domain, die Sie erstellen möchten.
   - *privateKey*Ersetzen Sie es durch Ihren privaten Schlüssel.

     > **Note**
     >
     > Sie müssen die erste und letzte Zeile (`-----BEGIN PRIVATE KEY-----` bzw. `-----END PRIVATE KEY-----`) des generierten privaten Schlüssels löschen. Darüber hinaus müssen Sie die Zeilenumbrüche im generierten privaten Schlüssel entfernen. Der resultierende Wert ist eine Zeichenfolge ohne Leerzeichen oder Zeilenumbrüche.

   - *selector*Ersetzen Sie ihn durch den eindeutigen Selektor, den Sie bei der Erstellung des TXT-Eintrags in der DNS-Konfiguration für Ihre Domain angegeben haben.

Wenn Sie fertig sind, speichern Sie die Datei unter `create-identity.json`.

2. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 create-email-identity --cli-input-json file://path/to/create-identity.json
```

Ersetzen Sie im vorherigen Befehl *path/to/create-identity.json* durch den vollständigen Pfad zu der Datei, die Sie im vorherigen Schritt erstellt haben.

Option 2: Konfigurieren einer vorhandenen Domänenidentität

Dieser Abschnitt enthält Verfahren zum Aktualisieren einer vorhandenen Domänenidentität für die Verwendung von BYODKIM. Eine vorhandene Domänenidentität ist eine Domäne, die Sie bereits zum Senden von E-Mails über Amazon SES eingerichtet haben.

So aktualisieren Sie eine Domänenidentität mit BYODKIM aus der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten eine Identität aus, in der Identity type (Identitätstyp) Domain (Domäne) ist.

> **Note**
>
> Informationen zum Erstellen oder Überprüfen einer Domäne finden Sie unter Erstellen einer Domänenidentität aus.

4. Wählen Sie auf der Registerkarte Authentifizierung im Bereich DomainKeys Identifizierte E-Mails (DKIM) die Option Bearbeiten aus.
5. Wählen Sie im Bereich Advanced DKIM settings (Erweiterte DKIM-Einstellungen) die Schaltfläche Provide DKIM authentication token (BYODKIM) (DKIM-Authentifizierungstoken bereitstellen (BYODKIM)) im Feld Identity type (Identitätstyp) aus.
6. Fügen Sie im Feld Private Key (Privater Schlüssel) den privaten Schlüssel ein, den Sie zuvor generiert haben.

> **Note**
>
> Sie müssen die erste und letzte Zeile (`-----BEGIN PRIVATE KEY-----` bzw. `-----END PRIVATE KEY-----`) des generierten privaten Schlüssels löschen. Darüber hinaus müssen Sie die Zeilenumbrüche im generierten privaten Schlüssel entfernen. Der resultierende Wert ist eine Zeichenfolge ohne Leerzeichen oder Zeilenumbrüche.

7. Geben Sie für Selector name (Name des Selektors) den Namen des Selektors ein, den Sie in den DNS-Einstellungen Ihrer Domäne angegeben haben.
8. Im Feld DKIM signatures (DKIM-Unterschriften) aktivieren Sie das Kontrollkästchen Enabled (Aktiviert).
9. Wählen Sie Änderungen speichern aus.

Um eine Domänenidentität mit BYODKIM zu aktualisieren, klicken Sie auf AWS CLI

Verwenden Sie die Operation `PutEmailIdentityDkimSigningAttributes` in der Amazon-SES-API, um eine neue Domäne einzurichten.

1. Fügen Sie folgenden Code in einen Texteditor ein:

```
{
    "SigningAttributes":{
        "DomainSigningPrivateKey":"privateKey",
        "DomainSigningSelector":"selector"
    },
    "SigningAttributesOrigin":"EXTERNAL"
}
```

   Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

   - Ersetzen Sie es durch *`privateKey`* Ihren privaten Schlüssel.

     > **Note**
     >
     > Sie müssen die erste und letzte Zeile (`-----BEGIN PRIVATE KEY-----` bzw. `-----END PRIVATE KEY-----`) des generierten privaten Schlüssels löschen. Darüber hinaus müssen Sie die Zeilenumbrüche im generierten privaten Schlüssel

entfernen. Der resultierende Wert ist eine Zeichenfolge ohne Leerzeichen oder Zeilenumbrüche.

- *selector*Ersetzen Sie ihn durch den eindeutigen Selektor, den Sie bei der Erstellung des TXT-Eintrags in der DNS-Konfiguration für Ihre Domain angegeben haben.

Wenn Sie fertig sind, speichern Sie die Datei unter `update-identity.json`.

2. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 put-email-identity-dkim-signing-attributes --email-identity example.com
 --cli-input-json file://path/to/update-identity.json
```

Nehmen Sie im vorherigen Befehl die folgenden Änderungen vor:

- *path/to/update-identity.json*Ersetzen Sie durch den vollständigen Pfad zu der Datei, die Sie im vorherigen Schritt erstellt haben.
- *example.com*Ersetzen Sie durch die Domain, die Sie aktualisieren möchten.

Überprüfen des DKIM-Status für eine Domäne, die BYODKIM verwendet

So überprüfen Sie den DKIM-Status einer Domäne über die Konsole

Nachdem Sie eine Domäne für die Verwendung von BYODKIM konfiguriert haben, können Sie mithilfe der SES-Konsole überprüfen, ob DKIM ordnungsgemäß konfiguriert wurde.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, deren DKIM-Status Sie überprüfen möchten.
4. Es kann bis zu 72 Stunden dauern, bis Änderungen an den DNS-Einstellungen weitergegeben werden. Sobald Amazon SES alle dieser DKIM-Einträge in der DNS-Konfiguration Ihrer Domäne erkennt, ist der Überprüfungsprozess abgeschlossen. Wenn alles korrekt konfiguriert wurde, wird im Feld DKIM-Konfiguration Ihrer Domain im Bereich DomainKeysIdentifizierte E-Mails (DKIM) der Wert Erfolgreich angezeigt, und im Feld Identitätsstatus wird im Übersichtsbereich Verifiziert angezeigt.

Um den DKIM-Status einer Domain zu überprüfen, verwenden Sie AWS CLI

Nachdem Sie eine Domain für die Verwendung von BYODKIM konfiguriert haben, können Sie den GetEmailIdentity Vorgang verwenden, um zu überprüfen, ob DKIM ordnungsgemäß konfiguriert ist.

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws sesv2 get-email-identity --email-identity example.com
  ```

  Ersetzen *example.com* Sie im vorherigen Befehl durch Ihre Domain.

  Dieser Befehl gibt ein JSON-Objekt zurück, das einen Abschnitt enthält, der dem folgenden Beispiel ähnelt.

  ```
  {
      ...
      "DkimAttributes": {
          "SigningAttributesOrigin": "EXTERNAL",
          "SigningEnabled": true,
          "Status": "SUCCESS",
          "Tokens": [ ]
      },
      ...
  }
  ```

  Wenn alle der folgenden Bedingungen zutreffen, ist BYODKIM für die Domäne richtig konfiguriert:

  - Der Wert der Eigenschaft `SigningAttributesOrigin` lautet `EXTERNAL`.
  - Der Wert von `SigningEnabled` ist `true`.
  - Der Wert von `Status` ist `SUCCESS`.

Verwaltung von Easy DKIM und BYODKIM

Sie können die DKIM-Einstellungen für Ihre Identitäten, die entweder mit Easy DKIM oder BYODKIM authentifiziert wurden, mit der webbasierten Amazon-SES-Konsole oder mit der Amazon-SES-API verwalten. Sie können beide Methoden verwenden, um die DKIM-Datensätze für eine Identität abzurufen oder DKIM-Signierung für eine Identität zu aktivieren oder zu deaktivieren.

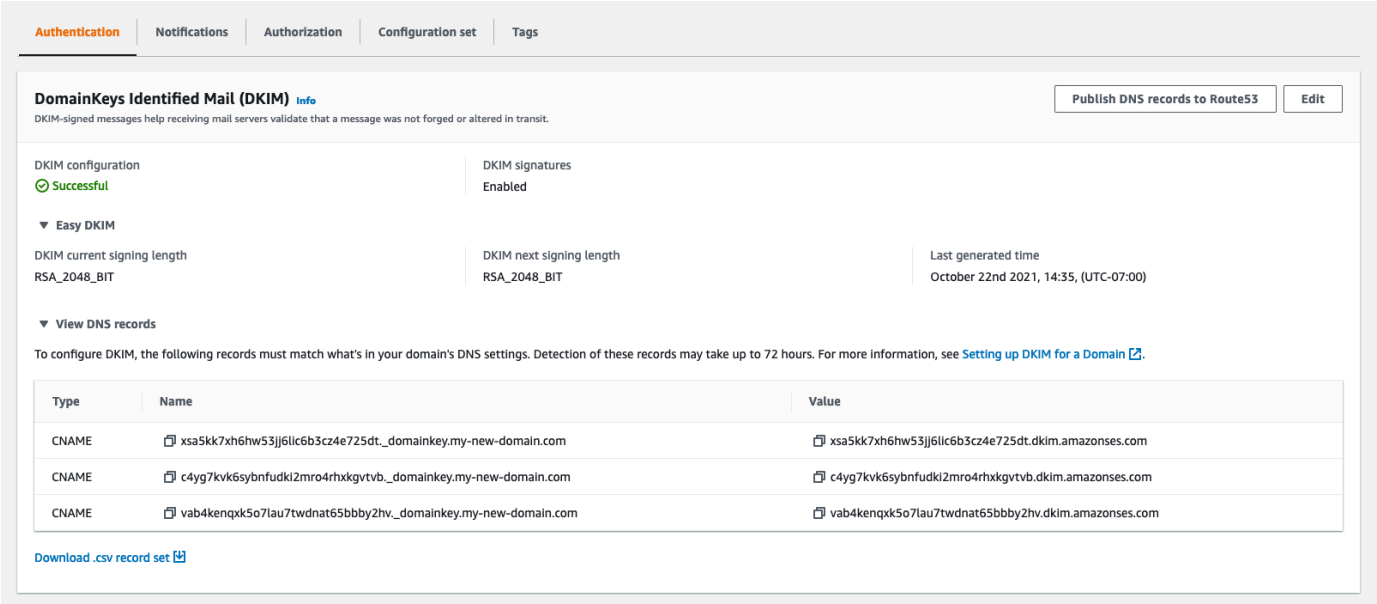
Abrufen von DKIM-Datensätzen für eine Identität

Sie können die DKIM-Datensätze für Ihre Domäne oder E-Mail-Adresse jederzeit mit der Amazon-SES-Konsole abrufen.

So rufen Sie die DKIM-Datensätze für eine Identität mit der Konsole ab

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie DKIM-Datensätze abrufen möchten.
4. Auf der Registerkarte Authentication (Authentifizierung) der Seite „Identitätsdetails“, erweitern Sie View DNS records (DNS-Datensätze anzeigen).
5. Kopieren Sie entweder die drei CNAME-Datensätze, wenn Sie Easy DKIM verwendet haben, oder den TXT-Datensatz, wenn Sie BYODKIM verwendet haben, die in diesem Abschnitt angezeigt werden. Alternativ können Sie Download Record Set as CSV (Datensatz als CSV-Datei herunterladen) auswählen, um eine Kopie der Datensätze auf Ihrem Computer zu speichern.

   Die folgende Abbildung enthält ein Beispiel für den erweiterten Abschnitt Anzeigen von DNS-Datensätzen, der mit Easy DKIM verbundene CNAME-Datensätze zeigt.



Sie können die DKIM-Datensätze für eine Identität auch mit der Amazon-SES-API abrufen. Eine gängige Methode, um mit der API zu interagieren, ist die Nutzung der AWS CLI.

Um die DKIM-Einträge für eine Identität abzurufen, verwenden Sie den AWS CLI

1. Geben Sie in der Befehlszeile folgenden Befehl ein:

   ```
   aws ses get-identity-dkim-attributes --identities "example.com"
   ```

   Ersetzen Sie dies im vorherigen Beispiel *example.com* durch die Identität, für die Sie DKIM-Einträge abrufen möchten. Sie können entweder eine E-Mail-Adresse oder eine Domäne angeben.

2. Die Ausgabe dieses Befehls enthält einen Abschnitt `DkimTokens`, wie im folgenden Beispiel gezeigt:

   ```
   {
       "DkimAttributes": {
           "example.com": {
               "DkimEnabled": true,
               "DkimVerificationStatus": "Success",
               "DkimTokens": [
                   "hirjd4exampled5477y22yd23ettobi",
                   "v3rnz522czcl46quexamplek3efo5o6x",
                   "y4examplexbhyhnsjcmtvzotfvqjmdqoj"
               ]
           }
       }
   }
   ```

   Sie können mit den Tokens CNAME-Datensätze erstellen, die Sie zu den DNS-Einstellungen für Ihre Domäne hinzufügen. Verwenden Sie zum Erstellen der CNAME-Datensätze die folgende Vorlage:

   ```
   token1._domainkey.example.com CNAME token1.dkim.amazonses.com
   token2._domainkey.example.com CNAME token2.dkim.amazonses.com
   token3._domainkey.example.com CNAME token3.dkim.amazonses.com
   ```

   Ersetzen Sie jede Instanz von *token1* durch das erste Token in der Liste, das Sie bei der Ausführung des `get-identity-dkim-attributes` Befehls erhalten haben, ersetzen Sie

alle Instanzen von *token2* durch das zweite Token in der Liste und alle Instanzen von *token3* durch das dritte Token in der Liste.

Beispiel: Wenn diese Vorlage auf die im vorhergehenden Beispiel gezeigten Token angewendet wird, werden die folgenden Datensätze erzeugt:

```
hirjd4exampled5477y22yd23ettobi._domainkey.example.com CNAME
 hirjd4exampled5477y22yd23ettobi.dkim.amazonses.com
v3rnz522czcl46quexamplek3efo5o6x._domainkey.example.com CNAME
 v3rnz522czcl46quexamplek3efo5o6x.dkim.amazonses.com
y4examplexbhyhnsjcmtvzotfvqjmdqoj._domainkey.example.com CNAME
 y4examplexbhyhnsjcmtvzotfvqjmdqoj.dkim.amazonses.com
```

> **Note**
>
> Nicht alle AWS-Regionen verwenden die standardmäßige SES-DKIM-Domain. `dkim.amazonses.com` Um zu sehen, ob Ihre Region eine regionsspezifische DKIM-Domain verwendet, schauen Sie in der Tabelle mit den DKIM-Domänen nach. Allgemeine AWS-Referenz

Deaktivieren von Easy DKIM für eine Identität

Sie können die DKIM-Authentifizierung für eine Identität mit der Amazon-SES-Konsole schnell deaktivieren.

So deaktivieren Sie DKIM für eine Identität

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie DKIM deaktivieren möchten.
4. Wählen Sie auf der Registerkarte Authentifizierung im Container DomainKeysIdentified Mail (DKIM) die Option Bearbeiten aus.
5. Deaktivieren Sie in Advanced DKIM settings (Erweiterte DKIM-Einstellungen) das Kontrollkästchen Enabled (Aktiviert) im Feld DKIM signatures (DKIM-Signaturen).

Sie können DKIM für eine Identität auch mit der Amazon-SES-API deaktivieren. Eine gängige Methode, um mit der API zu interagieren, ist die Nutzung der AWS CLI.

Um DKIM für eine Identität zu deaktivieren, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses set-identity-dkim-enabled --identity example.com --no-dkim-enabled
```

  Ersetzen Sie es im vorherigen Beispiel *example.com* durch die Identität, für die Sie DKIM deaktivieren möchten. Sie können entweder eine E-Mail-Adresse oder eine Domäne angeben.

Aktivieren von Easy DKIM für eine Identität

Wenn Sie DKIM für eine Identität zuvor deaktiviert haben, können Sie es über die Amazon-SES-Konsole erneut aktivieren.

So aktivieren Sie DKIM für eine Identität

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie DKIM aktivieren möchten.
4. Wählen Sie auf der Registerkarte Authentifizierung im Container DomainKeysIdentified Mail (DKIM) die Option Bearbeiten aus.
5. Prüfen Sie in Advanced DKIM settings (Erweiterte DKIM-Einstellungen) das Kontrollkästchen Enabled (Aktiviert) im Feld DKIM signatures (DKIM-Signaturen).

Sie können DKIM für eine Identität auch mit der Amazon-SES-API aktivieren. Eine gängige Methode, um mit der API zu interagieren, ist die Nutzung der AWS CLI.

Um DKIM für eine Identität zu aktivieren, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses set-identity-dkim-enabled --identity example.com --dkim-enabled
```

Ersetzen Sie dies im vorherigen Beispiel *example.com* durch die Identität, für die Sie DKIM aktivieren möchten. Sie können entweder eine E-Mail-Adresse oder eine Domäne angeben.

Überschreiben der geerbten DKIM-Signatur für eine E-Mail-Adressenidentität

In diesem Abschnitt erfahren Sie, wie Sie die geerbten DKIM-Signatureigenschaften der übergeordneten Domäne für eine bestimmte E-Mail-Adressenidentität, die Sie bereits mit Amazon SES überprüft haben, überschreiben (deaktivieren oder aktivieren). Sie können dies nur für E-Mail-Adressenidentitäten tun, die zu Domänen gehören, die Sie bereits besitzen, da DNS-Einstellungen auf Domänenebene konfiguriert sind.

Important

Sie können keine disable/enable DKIM-Signaturen für E-Mail-Adressidentitäten signieren...

- auf Domänen, die Sie nicht besitzen, nicht deaktivieren/aktivieren. Sie können beispielsweise die DKIM-Signatur für eine gmail.com- oder hotmail.com-Adresse nicht umschalten,
- auf Domänen, die Sie besitzen, aber in Amazon SES noch nicht überprüft wurden, nicht deaktivieren/aktivieren
- auf Domänen, die Sie besitzen, aber die DKIM-Signatur für die Domäne nicht aktiviert haben, nicht deaktivieren/aktivieren.

In diesem Abschnitt werden folgende Themen behandelt:

- Verstehen geerbter DKIM-Signatureigenschaften
- Überschreiben der DKIM-Signatur für eine E-Mail-Adressenidentität (Konsole)
- Überschreiben der DKIM-Signatur für eine E-Mail-Adressenidentität (AWS CLI)

Verstehen geerbter DKIM-Signatureigenschaften

Es ist wichtig, zuerst zu verstehen, dass eine E-Mail-Adressenidentität ihre DKIM-Signatureigenschaften von ihrer übergeordneten Domäne erbt, wenn diese Domäne mit DKIM konfiguriert wurde, unabhängig davon, ob Easy DKIM oder BYODKIM verwendet wurde. Daher ist das Deaktivieren oder Aktivieren der DKIM-Signatur für die E-Mail-Adressenidentität in Kraft, wodurch

die DKIM-Signatureigenschaften der Domäne basierend auf diesen wichtigen Fakten außer Kraft gesetzt werden:

- Wenn Sie DKIM bereits für die Domäne eingerichtet haben, zu der eine E-Mail-Adresse gehört, müssen Sie die DKIM-Signierung nicht auch für die E-Mail-Adressenidentität aktivieren.
  - Wenn Sie DKIM für eine Domäne einrichten, authentifiziert Amazon SES automatisch jede E-Mail von jeder Adresse in dieser Domäne über die geerbten DKIM-Eigenschaften der übergeordneten Domäne.
- DKIM-Einstellungen für eine bestimmte E-Mail-Adressenidentität überschreiben automatisch die Einstellungen der übergeordneten Domäne oder Unterdomäne (sofern zutreffend), zu der die Adresse gehört.

Da die DKIM-Signatureigenschaften der E-Mail-Adressenidentität von der übergeordneten Domäne geerbt werden, müssen Sie, wenn Sie diese Eigenschaften überschreiben möchten, die hierarchischen Regeln für das Überschreiben beachten, wie in der folgenden Tabelle beschrieben.

Die übergeordnete Domäne hat die DKIM-Signatur nicht aktiviert	Die übergeordnete Domäne hat die DKIM-Signatur aktiviert
Sie können die DKIM-Signatur für die E-Mail-Adressenidentität nicht aktivieren.	Sie können die DKIM-Signatur für die E-Mail-Adressenidentität deaktivieren.
	Sie können die DKIM-Signatur für die E-Mail-Adressenidentität erneut aktivieren.

Es wird im Allgemeinen nie empfohlen, Ihre DKIM-Signierung zu deaktivieren, da die Gefahr besteht, dass Ihre Senderreputation beeinträchtigt wird und es das Risiko erhöht, dass Ihre gesendeten E-Mails in Junk- oder Spam-Ordner wandern oder Ihre Domäne manipuliert wird.

Es besteht jedoch die Möglichkeit, die von der Domäne geerbten DKIM-Signatureigenschaften für eine E-Mail-Adressenidentität für einen bestimmten Anwendungsfall oder außerhalb der Geschäftsentscheidung außer Kraft zu setzen, dass Sie möglicherweise die DKIM-Signatur dauerhaft oder vorübergehend deaktivieren oder sie zu einem späteren Zeitpunkt wieder aktivieren müssen.

Überschreiben der DKIM-Signatur für eine E-Mail-Adressenidentität (Konsole)

Das folgende SES-Konsolenverfahren erläutert, wie Sie die geerbten DKIM-Signatureigenschaften der übergeordneten Domäne für eine bestimmte E-Mail-Adressenidentität, die Sie bereits mit Amazon SES überprüft haben, überschreiben (deaktivieren oder aktivieren).

Zur disable/enable DKIM-Signatur für eine E-Mail-Adressidentität mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten eine Identität aus, in der Identitätstyp E-Mail-Adresse ist und zu einer Ihrer verifizierten Domains gehört.
4. Wählen Sie auf der Registerkarte Authentifizierung im Container DomainKeys Identified Mail (DKIM) die Option Bearbeiten aus.

   > **Note**
   >
   > Die Registerkarte Authentifizierung ist nur vorhanden, wenn die ausgewählte E-Mail-Adresse-Identität zu einer Domäne gehört, die bereits von SES verifiziert wurde. Wenn Sie Ihre Domain noch nicht verifiziert haben, siehe Erstellen einer Domänenidentität.

5. Deaktivieren Sie unter Erweiterte DKIM-Einstellungen im Feld DKIM-Signaturen das Kontrollkästchen Aktiviert, um die DKIM-Signatur zu deaktivieren, oder wählen Sie sie aus, um die DKIM-Signatur erneut zu aktivieren (falls sie zuvor überschrieben wurde).
6. Wählen Sie Änderungen speichern aus.

Überschreiben der DKIM-Signatur für eine E-Mail-Adressenidentität (AWS CLI)

Im folgenden Beispiel werden der API-Befehl AWS CLI with a SES und Parameter verwendet, die die geerbten DKIM-Signatureigenschaften der übergeordneten Domain für eine bestimmte E-Mail-Adresse, die Sie bereits mit SES verifiziert haben, außer Kraft setzen (deaktivieren oder aktivieren).

Zur disable/enable DKIM-Signatur für eine E-Mail-Adressidentität mit dem AWS CLI

- Angenommen, Sie besitzen die example.com-Domäne und Sie möchten die DKIM-Signatur für eine der E-Mail-Adressen der Domäne deaktivieren, geben Sie in der Befehlszeile den folgenden Befehl ein:

```
aws sesv2 put-email-identity-dkim-attributes --email-identity marketing@example.com
 --no-signing-enabled
```

  a. *marketing@example.com*Ersetzen Sie es durch die Identität der E-Mail-Adresse, für die Sie die DKIM-Signatur deaktivieren möchten.

  b. `--no-signing-enabled` wird die DKIM-Signatur deaktivieren. Zum erneuten Aktivieren der DKIM-Signatur verwenden Sie `--signing-enabled`.

Manuelle DKIM-Signierung in Amazon SES

Als Alternative zur Verwendung von Easy DKIM können Sie die DKIM-Signaturen auch manuell zu Ihren Nachrichten hinzufügen und diese Nachrichten anschließend mit Amazon SES versenden. Wenn Sie Ihre Nachrichten manuell signieren möchten, müssen Sie zunächst eine DKIM-Signatur erstellen. Nachdem Sie die Nachricht und die DKIM-Signatur erstellt haben, können Sie sie mit der SendRawEmailAPI senden.

Wenn Sie Ihre E-Mails manuell signieren möchten, beachten Sie die folgenden Aspekte:

- Jede Nachricht, die Sie mit Amazon SES versenden, enthält einen DKIM-Header, der auf eine Signaturdomäne von amazonses.com verweist (es ist also die folgende Zeichenfolge enthalten: `d=amazonses.com`). Wenn Sie Ihre Nachrichten manuell signieren, sollten Ihre Nachrichten zwei DKIM-Header enthalten: einen für Ihre Domäne und einen, den Amazon SES automatisch für amazonses.com erstellt.
- DKIM-Signaturen, die Sie manuell zu Ihren Nachrichten hinzufügen, werden von Amazon SES nicht validiert. Wenn in Zusammenhang mit der DKIM-Signatur in einer Nachricht Fehler auftreten, wird die Nachricht möglicherweise von E-Mail-Anbietern zurückgewiesen.
- Verwenden Sie beim Signieren Ihrer Nachrichten eine Bitlänge von mindestens 1024 Bits.
- Signieren Sie die folgenden Felder nicht: Message-ID, Date, Return-Path, Bounces-To.

> **Note**
>
> Wenn Sie Ihre E-Mails mit einem E-Mail-Client über die Amazon-SES-SMTP-Schnittstelle versenden, versieht der Client möglicherweise die Nachrichten automatisch mit DKIM-Signaturen. Einige Client signieren möglicherweise einige dieser Felder. Informationen dazu, welche Felder standardmäßig signiert sind, finden Sie in der Dokumentation zu Ihrem E-Mail-Client.

Authentifizierung Ihrer E-Mails mit SPF in Amazon SES

Sender Policy Framework (SPF) ist ein E-Mail-Validierungsstandard, der entwickelt wurde, um E-Mail-Spoofing zu verhindern. Domänenbesitzer verwenden SPF, um E-Mail-Anbietern mitzuteilen, welche Server E-Mails von ihren Domänen senden dürfen. SPF ist in RFC 7208 definiert.

Nachrichten, die über Amazon SES gesendet werden, verwenden automatisch eine Subdomain von `amazonses.com` als standardmäßige MAIL-FROM-Domain verwendet. Die SPF-Authentifizierung verifiziert diese Nachrichten erfolgreich, da die standardmäßige MAIL-FROM-Domain mit dem sendenden Mail-Server, SES, übereinstimmt. Daher ist SPF in SES implizit für Sie eingerichtet.

Wenn Sie jedoch nicht die SES-Standarddomäne MAIL FROM verwenden möchten, sondern lieber eine Subdomain einer Domain verwenden möchten, die Sie besitzen, wird dies in SES als Verwendung einer benutzerdefinierten MAIL FROM-Domäne bezeichnet. Dazu müssen Sie Ihren eigenen SPF-Datensatz für Ihre benutzerdefinierte MAIL-FROM-Domain veröffentlichen. Außerdem erfordert SES, dass Sie einen MX-Datensatz einrichten, damit Ihre benutzerdefinierte MAIL-FROM-Domain die Unzustellbarkeits- und Beschwerdebenachrichtigungen erhält, die E-Mail-Anbieter Ihnen senden.

Erfahren Sie, wie Sie die SPF-Authentifizierung einrichten

Es werden Anweisungen zur Konfiguration Ihrer Domain mit SPF und zum Veröffentlichen der MX- und SPF-Einträge (Typ TXT) gegeben. the section called “Verwenden einer benutzerdefinierten MAIL FROM-Domäne”

Verwenden einer benutzerdefinierten MAIL FROM-Domäne

Wenn eine E-Mail gesendet wird, enthält sie zwei Adressen zur Angabe ihrer Quelle: eine From-Adresse, die dem Empfänger der Nachricht angezeigt wird, und eine MAIL FROM-Adresse, die angibt, woher die Nachricht stammt. Die MAIL FROM-Adresse wird auch als envelope sender,

envelope from, bounce address, oder Return-Path-Adresse bezeichnet. Mail-Server verwenden die MAIL FROM-Adresse, um Unzustellbarkeitsnachrichten und andere Fehlerbenachrichtigungen zurückzugeben. Die MAIL FROM-Adresse kann für Empfänger in der Regel nur angezeigt werden, wenn sie den Quellcode für die Nachricht anzeigen.

Amazon SES legt die MAIL-FROM-Domain für die Nachrichten, die Sie senden, auf einen Standardwert fest, es sei denn, Sie geben Ihre eigene (benutzerdefinierte) Domain an. Dieser Abschnitt erläutert die Vorteile der Einrichtung einer benutzerdefinierten MAIL FROM-Domäne und enthält Einrichtungsverfahren.

Warum sollten Sie eine benutzerdefinierte MAIL FROM-Domäne verwenden?

Nachrichten, die über Amazon SES gesendet werden, verwenden automatisch eine Subdomain von `amazonses.com` als standardmäßige MAIL-FROM-Domain verwendet. Die Sender Policy Framework(SPF)-Authentifizierung verifiziert diese Nachrichten erfolgreich, da die standardmäßige MAIL-FROM-Domain mit dem sendenden Mail-Server, in diesem Fall SES, übereinstimmt.

Wenn Sie nicht die SES-Standarddomain MAIL FROM verwenden möchten, sondern die Verwendung der Subdomain einer Domain, die Ihnen gehört, bevorzugen, wird dies in SES als Verwendung einer benutzerdefinierten MAIL-FROM-Domain bezeichnet. Dazu müssen Sie Ihren eigenen SPF-Datensatz für Ihre benutzerdefinierte MAIL-FROM-Domain veröffentlichen. Außerdem erfordert SES, dass Sie einen MX-Datensatz einrichten, damit Ihre Domain die Unzustellbarkeits- und Beschwerdebenachrichtigungen erhält, die E-Mail-Anbieter Ihnen senden.

Durch die Verwendung einer benutzerdefinierten MAIL-FROM-Domain haben Sie die Flexibilität, SPF, DKIM oder beides zu verwenden, um eine Validierung mit DMARC (Domain-based Message Authentication, Reporting and Conformance) zu erreichen. Mit DMARC kann die Domäne eines Senders angeben, dass von der Domäne gesendete E-Mails durch ein oder mehrere Authentifizierungssysteme geschützt sind. Es gibt zwei Möglichkeiten, eine DMARC-Validierung zu erreichen: the section called “Einhaltung von DMARC über SPF” und the section called “Einhaltung von DMARC über DKIM”.

Auswählen einer benutzerdefinierten MAIL-FROM-Domain

Im Folgenden bezieht sich der Begriff MAIL FROM-Domain immer auf eine Subdomain einer Domain, die Sie besitzen — diese Subdomain, die Sie für Ihre benutzerdefinierte MAIL FROM-Domain verwenden, darf für nichts anderes verwendet werden und erfüllt die folgenden Anforderungen:

- Die MAIL FROM-Domain muss eine Subdomain der übergeordneten Domain einer verifizierten Identität (E-Mail-Adresse oder Domain) sein.

- Die MAIL FROM-Domäne sollte keine Unterdomäne sein, von der Sie auch E-Mails senden.
- Bei der MAIL FROM-Domäne sollte es sich nicht um eine Unterdomäne handeln, auf der Sie E-Mails erhalten.

Verwenden von SPF mit Ihrer benutzerdefinierten MAIL-FROM-Domain

Sender Policy Framework (SPF) ist ein E-Mail-Validierungsstandard, der entwickelt wurde, um E-Mail-Spoofing zu verhindern. Sie können Ihre benutzerdefinierte MAIL-FROM-Domain mit SPF konfigurieren, um E-Mail-Anbietern mitzuteilen, welche Server E-Mails von Ihrer benutzerdefinierten MAIL-FROM-Domain senden dürfen. SPF ist in RFC 7208 definiert.

Zum Einrichten von SPF veröffentlichen Sie einen TXT-Datensatz in der DNS-Konfiguration für Ihre benutzerdefinierte MAIL-FROM-Domain. Dieser Datensatz enthält eine Liste der Server, die Sie zum Senden von E-Mails aus Ihrer benutzerdefinierten MAIL-FROM-Domain autorisieren. Wenn ein E-Mail-Anbieter eine Nachricht von Ihrer benutzerdefinierten MAIL-FROM-Domain empfängt, überprüft er die DNS-Datensätze für Ihre Domain darauf, ob die E-Mail von einem autorisierten Server gesendet wurde.

Wenn Sie diesen SPF-Datensatz verwenden möchten, um DMARC-konform zu sein, muss die Domain in der Absenderadresse mit der MAIL-FROM-Domain übereinstimmen. Siehe the section called “Einhaltung von DMARC über SPF”.

Im nächsten Abschnitt, the section called “Konfigurieren Ihrer benutzerdefinierten MAIL-FROM-Domain”, wird erklärt, wie Sie SPF für Ihre benutzerdefinierte MAIL-FROM-Domain einrichten.

Konfigurieren Ihrer benutzerdefinierten MAIL-FROM-Domain

Für die Einrichtung einer benutzerdefinierten MAIL FROM-Domäne müssen Sie Datensätze zur DNS-Konfiguration für die Domäne hinzufügen. SES verlangt von Ihnen, dass Sie einen MX-Eintrag veröffentlichen, damit Ihre Domain die Bounce- und Beschwerdebenachrichtigungen erhalten kann, die Ihnen E-Mail-Anbieter senden. Sie müssen auch einen SPF-Datensatz (Typ TXT) veröffentlichen, um nachzuweisen, dass Amazon SES berechtigt ist, E-Mails von Ihrer Domäne zu senden.

Sie können eine benutzerdefinierte MAIL FROM-Domain für eine gesamte Domain oder Subdomain sowie für einzelne E-Mail-Adressen einrichten. Die folgenden Verfahren zeigen, wie Sie mit der Amazon-SES-Konsole eine benutzerdefinierte MAIL FROM-Domäne konfigurieren. Sie können eine benutzerdefinierte MAIL FROM-Domain auch mithilfe der SetIdentityMailFromDomainAPI-Operation konfigurieren.

Einrichten einer benutzerdefinierten MAIL-FROM-Domain für eine verifizierte Domain

Diese Verfahren zeigen Ihnen, wie Sie eine benutzerdefinierte MAIL FROM-Domäne für eine gesamte Domain oder Subdomain konfigurieren, sodass alle Nachrichten, die von Adressen in dieser Domain gesendet werden, diese benutzerdefinierte MAIL FROM-Domäne verwenden.

So konfigurieren Sie eine verifizierte Domäne für die Verwendung einer bestimmten benutzerdefinierten MAIL FROM-Domäne

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, die Sie konfigurieren möchten, wobei der Identity type (Identitätstyp) Domain (Domäne) und der Status Verified (Verifiziert) ist.
   - Wenn der Status Unverified (Nicht verifiziert) ist, führen Sie die Verfahren unter Verifizieren einer DKIM-Domänenidentität bei Ihrem DNS-Anbieter aus, um die Domäne der E-Mail-Adresse zu überprüfen.
4. Wählen Sie unten auf dem Bildschirm im Bereich Custom MAIL FROM domain die Option Bearbeiten aus.
5. Gehen Sie im Bereich General details (Allgemeine Details) wie folgt vor:
   a. Wählen Sie das Kontrollkästchen Use a custom MAIL FROM domain (Verwenden einer benutzerdefinierten MAIL-FROM-Domäne).
   b. Geben Sie für MAIL FROM domain (MAIL FROM-Domäne) die Subdomäne ein, die Sie als MAIL FROM-Domäne verwenden möchten.
   c. Wählen Sie für Behavior on MX failure (Verhalten bei MX-Fehler) eine der folgenden Optionen aus:
      - Standard-MAIL-FROM-Domäne verwenden – Wenn der MX-Datensatz der benutzerdefinierten MAIL-FROM-Domäne nicht richtig eingerichtet ist, verwendet Amazon SES eine Unterdomäne von `amazonses.com`. Die Subdomain hängt davon ab AWS-Region , in welcher Sie Amazon SES verwenden.
      - Nachricht ablehnen – Wenn ein benutzerdefinierter MX-Eintrag der MAIL FROM-Domäne nicht ordnungsgemäß eingerichtet ist, gibt Amazon SES einen `MailFromDomainNotVerified`-Fehler zurück. E-Mails, die Sie von dieser Domäne aus senden möchten, werden automatisch abgelehnt.

d. Wählen Sie Save changes (Änderungen speichern) aus. Sie kehren zum vorherigen Bildschirm zurück.

6. Veröffentlichen Sie die MX- und SPF-Datensätze (Typ TXT) im DNS-Server der benutzerdefinierten MAIL FROM-Domäne:

   Im Bereich Custom MAIL FROM domain (Benutzerdefinierte MAIL FROM-Domäne) der Tabelle Publish DNS records (DNS-Datensätze veröffentlichen) werden jetzt die MX- und SPF-Datensätze (Typ TXT) angezeigt, die Sie an die DNS-Konfiguration Ihrer Domäne veröffentlichen (ihr hinzufügen) müssen. Diese Datensätze verwenden die Formate in der folgenden Tabelle.

Name	Typ	Wert
subdomain .*domain*.*com*	MX	10 feedback-smtp.*region*.amazonses.com
subdomain .*domain*.*com*	TXT	„v=spf1include:amazonses.com~all“

   In den vorhergehenden Datensätzen wird

   - *subdomain*. *domain*. *com*wird mit Ihrer MAIL FROM-Subdomain gefüllt
   - *region*wird mit dem Namen der Domain aufgefüllt, für die AWS-Region Sie die MAIL FROM-Domain verifizieren möchten (z. B. `us-west-2us-east-1`,`eu-west-1`, oder usw.)
   - Die Zahl 10, die zusammen mit dem MX-Wert aufgeführt ist, ist die Präferenzreihenfolge für den Mailserver und muss in ein separates Wertefeld eingegeben werden, wie von der GUI Ihres DNS-Anbieters angegeben.
   - Der TXT-Eintragswert des SPF muss normalerweise die Anführungszeichen enthalten, aber einige DNS-Anbieter verlangen sie nicht.

   Kopieren Sie aus der Tabelle Publish DNS records (DNS-Datensätze veröffentlichen) die MX- und SPF-Datensätze (Typ TXT), indem Sie das Kopiersymbol neben jedem Wert auswählen und in die entsprechenden Felder der GUI Ihres DNS-Anbieters einfügen. Alternativ können Sie Download Record Set as CSV (Datensatz als CSV-Datei herunterladen) auswählen, um eine Kopie der Datensätze auf Ihrem Computer zu speichern.

> **Important**
>
> - Die spezifischen Verfahren für die Veröffentlichung der MX- und SPF-Einträge (Typ TXT) hängen von Ihrem DNS- oder Hosting-Anbieter ab. Informationen zum Hinzufügen dieser Einträge zur DNS-Konfiguration für Ihre Domain erhalten Sie in der Dokumentation Ihres Anbieters oder kontaktieren Sie ihn.
> - Um erfolgreich eine benutzerdefinierte MAIL FROM-Domäne mit Amazon SES einzurichten, müssen Sie genau einen MX-Datensatz im DNS-Server Ihrer benutzerdefinierten MAIL FROM-Domäne veröffentlichen. Wenn die MAIL FROM-Domäne über mehrere MX-Datensatz verfügt, wird die benutzerdefinierte MAIL FROM-Einrichtung mit Amazon SES fehlschlagen.

Wenn Route 53 den DNS-Dienst für Ihre MAIL FROM-Domäne bereitstellt und Sie mit demselben Konto angemeldet sind, das Sie für Route 53 verwenden, wählen Sie „Datensätze mit Route 53 veröffentlichen“. AWS-Managementkonsole Die DNS-Datensätze werden automatisch auf die DNS-Konfiguration Ihrer Domäne angewendet.

Wenn Sie einen anderen DNS-Anbieter verwenden, müssen Sie die DNS-Datensätze manuell auf dem DNS-Server der MAIL FROM-Domäne veröffentlichen. Das Verfahren zum Hinzufügen von DNS-Datensätzen zum DNS-Server Ihrer Domäne variiert je nach Webhosting-Service oder DNS-Anbieter.

Die Verfahren für die Veröffentlichung von DNS-Datensätzen für Ihre Domäne hängen davon ab, welchen DNS-Anbieter Sie verwenden. Die folgende Tabelle enthält Links zur Dokumentation für einige gängige DNS-Anbieter. Diese Liste ist nicht vollständig und stellt keine Empfehlung dar. Wenn Ihr DNS-Anbieter nicht aufgeführt ist, bedeutet dies nicht, dass er die MAIL FROM-Domänenkonfiguration nicht unterstützt.

Name des DNS/Hosting-Anbieters	Link zur Dokumentation
GoDaddy	• MX: Hinzufügen eines MX-Datensatzes (externer Link) • TXT: Hinzufügen eines TXT-Datensatzes (externer Link)

Name des DNS/Hosting-Anbieters	Link zur Dokumentation
DreamHost	• MX: Wie ändere ich meine MX-Datensätze? (externer Link) • TXT: Wie füge ich benutzerdefinierte DNS-Datensätze hinzu? (externer Link)
Cloudflare	• MX: Wie kann ich Mail- oder MX-Datensätze hinzufügen oder bearbeiten? (externer Link) • TXT: Verwalten von DNS-Datensätzen in CloudFlare (externer Link)
HostGator	• MX: Einrichten von E-Mail-Datensätzen (externer Link) • TXT: DNS-Einträge mit HostGator /eNOM verwalten (externer Link)
Namecheap	• MX: Wie kann ich die für den Mail-Service benötigten MX-Datensätze einrichten? (externer Link) • TXT: Wie füge ich TXT/SPF/DKIM/DMARC Einträge für meine Domain hinzu? (externer Link)
Names.co.uk	• MX: Ändern der DNS-Einstellungen Ihrer Domäne (externer Link) • TXT: Ändern der DNS-Einstellungen Ihrer Domänen (externer Link)
Wix	• MX: Hinzufügen oder Aktualisieren von MX-Datensätzen in Ihrem Wix-Konto (externer Link) • TXT: Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto (externer Link)

Wenn Amazon SES feststellt, dass die Datensätze vorhanden sind, erhalten Sie eine E-Mail, in der Sie darüber informiert werden, dass Ihre benutzerdefinierte MAIL FROM-Domäne erfolgreich eingerichtet wurde. Abhängig von Ihrem DNS-Anbieter kann es zu einer Verzögerung von bis zu 72 Stunden kommen, bevor Amazon SES den MX-Eintrag erkennt.

Einrichten einer benutzerdefinierten MAIL-FROM-Domain für eine verifizierte E-Mail-Adresse

Sie können auch eine benutzerdefinierte MAIL FROM-Domäne für eine bestimmte E-Mail-Adresse einrichten. Um eine benutzerdefinierte MAIL FROM Domäne für eine E-Mail-Adresse einrichten zu können, müssen Sie zum Ändern der DNS-Datensätze für die Domäne, der die E-Mail-Adresse zugeordnet ist, berechtigt sein.

> **Note**
>
> Sie können keine benutzerdefinierte MAIL FROM-Domäne für Adressen in einer Domäne einrichten, die Sie nicht besitzen (Sie können beispielsweise keine benutzerdefinierte MAIL FROM-Domäne für eine Adresse in der Domäne `gmail.com` erstellen, da Sie der Domäne die erforderlichen DNS-Datensätze nicht hinzufügen können).

So konfigurieren Sie eine verifizierte E-Mail-Adresse, um eine festgelegte MAIL FROM-Domäne zu verwenden

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, die Sie konfigurieren möchten, wobei der Identity type (Identitätstyp) Email address (E-Mail-Adresse) und der Status Verified (Verifiziert) ist.
   - Wenn der Status Unverified Nicht verifiziert) ist, führen Sie die Verfahren unter Verifizieren der Identität einer E-Mail-Adresse aus, um die Domäne der E-Mail-Adresse zu überprüfen.
4. Wählen Sie auf der Registerkarte MAIL FROM Domain (MAIL-FROM-Domäne) im Bereich Custom MAIL FROM domain (Benutzerdefinierte MAIL-FROM-Domäne) Edit (Bearbeiten) aus.
5. Gehen Sie im Bereich General details (Allgemeine Details) wie folgt vor:

a. Wählen Sie das Kontrollkästchen Use a custom MAIL FROM domain (Verwenden einer benutzerdefinierten MAIL-FROM-Domäne).

b. Geben Sie für MAIL FROM domain (MAIL FROM-Domäne) die Subdomäne ein, die Sie als MAIL FROM-Domäne verwenden möchten.

c. Wählen Sie für Behavior on MX failure (Verhalten bei MX-Fehler) eine der folgenden Optionen aus:

   - Standard-MAIL-FROM-Domäne verwenden – Wenn der MX-Datensatz der benutzerdefinierten MAIL-FROM-Domäne nicht richtig eingerichtet ist, verwendet Amazon SES eine Unterdomäne von `amazonses.com`. Die Subdomain hängt davon ab AWS-Region , in welcher Sie Amazon SES verwenden.
   - Nachricht ablehnen – Wenn ein benutzerdefinierter MX-Eintrag der MAIL FROM-Domäne nicht ordnungsgemäß eingerichtet ist, gibt Amazon SES einen `MailFromDomainNotVerified`-Fehler zurück. E-Mails werden bei einem Sendeversuch von dieser Adresse automatisch abgelehnt.

d. Wählen Sie Save changes (Änderungen speichern) aus. Sie kehren zum vorherigen Bildschirm zurück.

6. Veröffentlichen Sie die MX- und SPF-Datensätze (Typ TXT) im DNS-Server der benutzerdefinierten MAIL FROM-Domäne:

   Im Bereich Custom MAIL FROM domain (Benutzerdefinierte MAIL FROM-Domäne) der Tabelle Publish DNS records (DNS-Datensätze veröffentlichen) werden jetzt die MX- und SPF-Datensätze (Typ TXT) angezeigt, die Sie an die DNS-Konfiguration Ihrer Domäne veröffentlichen (ihr hinzufügen) müssen. Diese Datensätze verwenden die Formate in der folgenden Tabelle.

Name	Typ	Wert
subdomain .*domain*.*com*	MX	10 feedback-smtp.*region*.amazonses.com
subdomain .*domain*.*com*	TXT	„v=spf1include:amazonses.com~all“

   In den vorhergehenden Datensätzen wird

- *subdomain*. *domain*. *com*wird mit Ihrer MAIL FROM-Subdomain gefüllt
- *region*wird mit dem Namen der Domain aufgefüllt, für die AWS-Region Sie die MAIL FROM-Domain verifizieren möchten (z. B. `us-west-2`us-east-1,`eu-west-1`, oder usw.)
- Die Zahl 10, die zusammen mit dem MX-Wert aufgeführt ist, ist die Präferenzreihenfolge für den Mailserver und muss in ein separates Wertefeld eingegeben werden, wie von der GUI Ihres DNS-Anbieters angegeben.
- Der Wert des SPF TXT-Datensatzes muss die Anführungszeichen enthalten.

Kopieren Sie aus der Tabelle Publish DNS records (DNS-Datensätze veröffentlichen) die MX- und SPF-Datensätze (Typ TXT), indem Sie das Kopiersymbol neben jedem Wert auswählen und in die entsprechenden Felder der GUI Ihres DNS-Anbieters einfügen. Alternativ können Sie Download Record Set as CSV (Datensatz als CSV-Datei herunterladen) auswählen, um eine Kopie der Datensätze auf Ihrem Computer zu speichern.

> **Important**
>
> Um erfolgreich eine benutzerdefinierte MAIL FROM-Domäne mit Amazon SES einzurichten, müssen Sie genau einen MX-Datensatz im DNS-Server Ihrer benutzerdefinierten MAIL FROM-Domäne veröffentlichen. Wenn die MAIL FROM-Domäne über mehrere MX-Datensatz verfügt, wird die benutzerdefinierte MAIL FROM-Einrichtung mit Amazon SES fehlschlagen.

Wenn Route 53 den DNS-Dienst für Ihre MAIL FROM-Domäne bereitstellt und Sie mit demselben Konto angemeldet sind, das Sie für Route 53 verwenden, wählen Sie „Datensätze mit Route 53 veröffentlichen“. AWS-Managementkonsole Die DNS-Datensätze werden automatisch auf die DNS-Konfiguration Ihrer Domäne angewendet.

Wenn Sie einen anderen DNS-Anbieter verwenden, müssen Sie die DNS-Datensätze manuell auf dem DNS-Server der MAIL FROM-Domäne veröffentlichen. Das Verfahren zum Hinzufügen von DNS-Datensätzen zum DNS-Server Ihrer Domäne variiert je nach Webhosting-Service oder DNS-Anbieter.

Die Verfahren für die Veröffentlichung von DNS-Datensätzen für Ihre Domäne hängen davon ab, welchen DNS-Anbieter Sie verwenden. Die folgende Tabelle enthält Links zur Dokumentation für einige gängige DNS-Anbieter. Diese Liste ist nicht vollständig und stellt keine Empfehlung

dar. Wenn Ihr DNS-Anbieter nicht aufgeführt ist, bedeutet dies nicht, dass er die MAIL FROM-Domänenkonfiguration nicht unterstützt.

Name des DNS/Hosting-Anbieters	Link zur Dokumentation
GoDaddy	• MX: Hinzufügen eines MX-Datensatzes (externer Link) • TXT: Hinzufügen eines TXT-Datensatzes (externer Link)
DreamHost	• MX: Wie ändere ich meine MX-Datensätze? (externer Link) • TXT: Wie füge ich benutzerdefinierte DNS-Datensätze hinzu? (externer Link)
Cloudflare	• MX: Wie kann ich Mail- oder MX-Datensätze hinzufügen oder bearbeiten? (externer Link) • TXT: Verwalten von DNS-Datensätzen in CloudFlare (externer Link)
HostGator	• MX: Ändern von MX-Datensätzen – Windows (externer Link) • TXT: DNS-Einträge mit HostGator /eNOM verwalten (externer Link)
Namecheap	• MX: Wie kann ich die für den Mail-Service benötigten MX-Datensätze einrichten? (externer Link) • TXT: Wie füge ich TXT/SPF/DKIM/DMARC Einträge für meine Domain hinzu? (externer Link)

Name des DNS/Hosting-Anbieters	Link zur Dokumentation
Names.co.uk	• MX: Ändern der DNS-Einstellungen Ihrer Domäne (externer Link) • TXT: Ändern der DNS-Einstellungen Ihrer Domänen (externer Link)
Wix	• MX: Hinzufügen oder Aktualisieren von MX-Datensätzen in Ihrem Wix-Konto (externer Link) • TXT: Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto (externer Link)

Wenn Amazon SES feststellt, dass die Datensätze vorhanden sind, erhalten Sie eine E-Mail, in der Sie darüber informiert werden, dass Ihre benutzerdefinierte MAIL FROM-Domäne erfolgreich eingerichtet wurde. Abhängig von Ihrem DNS-Anbieter kann es zu einer Verzögerung von bis zu 72 Stunden kommen, bevor Amazon SES den MX-Eintrag erkennt.

Einrichtungszustände der benutzerdefinierten MAIL-FROM-Domain mit Amazon SES

Nach der Konfiguration einer Identität für die Verwendung einer benutzerdefinierten MAIL FROM-Domäne, wechselt der Einrichtungszustand zu "Pending" während Amazon SES versucht, den erforderlichen MX-Eintrag in Ihren DNS-Einstellungen zu erkennen. Der Zustand ändert sich daraufhin abhängig davon, ob Amazon SES den MX-Eintrag erkennt. Die folgende Tabelle beschreibt das E-Mail-Sendeverhalten und die jeweils entsprechenden Amazon-SES-Aktionen für die einzelnen Zustände. Jedes Mal, wenn sich der Status ändert, sendet Amazon SES eine Benachrichtigung an die E-Mail-Adresse, die mit Ihrem verknüpft ist AWS-Konto.

Status	E-Mail-Sendeverhalten	Amazon-SES-Aktionen
Ausstehend	Verwendet benutzerdefinierte MAIL FROM-Fallback-Einstellung	Amazon SES versucht, den erforderlichen MX-Eintrag für

Status	E-Mail-Sendeverhalten	Amazon-SES-Aktionen
		72 Stunden zu erkennen. Im Falle eines Fehlschlags ändert sich der Zustand zu "Failed".
Herzlichen Glückwunsch	Verwendet benutzerdefinierte MAIL FROM-Domäne	Amazon SES überprüft kontinuierlich, ob der erforderliche MX-Eintrag vorliegt.
Temporary Failure	Verwendet benutzerdefinierte MAIL FROM-Fallback-Einstellung	Amazon SES versucht, den erforderlichen MX-Eintrag für 72 Stunden zu erkennen. Im Falle eines Fehlschlags, ändert sich der Zustand zu "Failed". Wenn erfolgreich, ändert sich der Zustand zu "Success".

Status	E-Mail-Sendeverhalten	Amazon-SES-Aktionen
Fehlgeschlagen	Verwendet benutzerdefinierte MAIL FROM-Fallback-Einstellung	Amazon SES versucht nicht länger, den erforderlichen MX-Eintrag zu erkennen. Zum Verwenden einer benutzerdefinierten MAIL FROM-Domäne müssen Sie den Einrichtungsvorgang in Konfigurieren Ihrer benutzerdefinierten MAIL-FROM-Domain neu starten.

Einhaltung des DMARC-Authentifizierungsprotokolls in Amazon SES

Domain-based Message Authentication, Reporting and Conformance (DMARC) ist ein E-Mail-Authentifizierungsprotokoll, das Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) verwendet, um E-Mail-Spoofing und Phishing zu erkennen. Um DMARC-konform zu sein, müssen Nachrichten entweder über SPF oder DKIM authentifiziert werden. Wenn Sie jedoch beide mit DMARC verwenden, gewährleisten Sie im Idealfall den höchstmöglichen Schutz für Ihren E-Mail-Versand.

Schauen wir uns kurz an, was jeder tut und wie DMARC sie alle miteinander verbindet:

- SPF — Identifiziert, welche Mailserver E-Mails im Namen Ihrer benutzerdefinierten MAIL FROM-Domain über einen DNS-TXT-Eintrag senden dürfen, der von DNS verwendet wird. Die E-Mail-Systeme der Empfänger ermitteln anhand des SPF-TXT-Eintrags, ob eine Nachricht von Ihrer benutzerdefinierten Domain von einem autorisierten Messaging-Server stammt. Im Grunde soll

SPF helfen, Spoofing zu verhindern, aber es gibt Spoofing-Techniken, für die SPF in der Praxis anfällig ist, und aus diesem Grund müssen Sie DKIM zusammen mit DMARC verwenden.

- DKIM — Fügt Ihren ausgehenden Nachrichten im E-Mail-Header eine digitale Signatur hinzu. Empfangende E-Mail-Systeme können anhand dieser digitalen Signatur überprüfen, ob eingehende E-Mails mit einem Schlüssel signiert sind, der der Domain gehört. Wenn ein empfangendes E-Mail-System eine Nachricht weiterleitet, wird der Umschlag der Nachricht jedoch so geändert, dass die SPF-Authentifizierung ungültig wird. Da die digitale Signatur in der E-Mail-Nachricht verbleibt, weil sie Teil des E-Mail-Headers ist, funktioniert DKIM auch dann, wenn eine Nachricht zwischen Mailservern weitergeleitet wurde (sofern der Nachrichteninhalt nicht geändert wurde).
- DMARC — Stellt sicher, dass eine Domainabstimmung mit mindestens einem von SPF und DKIM besteht. Die alleinige Verwendung von SPF und DKIM gewährleistet nicht, dass die Absenderadresse authentifiziert ist (dies ist die E-Mail-Adresse, die Ihr Empfänger in seinem E-Mail-Client sieht). SPF überprüft nur die in der MAIL FROM-Adresse angegebene Domain (wird von Ihrem Empfänger nicht gesehen). DKIM überprüft nur die in der DKIM-Signatur angegebene Domain (auch nicht für Ihren Empfänger sichtbar). DMARC behebt diese beiden Probleme, indem es verlangt, dass die Domänenausrichtung entweder auf SPF oder DKIM korrekt ist:
  - Damit SPF das DMARC-Alignment bestehen kann, muss die Domain in der Absenderadresse mit der Domain in der MAIL FROM-Adresse (auch als Return-Path- und Envelope-From-Adresse bezeichnet) übereinstimmen. Dies ist bei weitergeleiteten E-Mails selten möglich, weil sie entfernt werden, oder beim Senden von E-Mails über externe Massen-E-Mail-Anbieter, weil der Return-Path (MAIL FROM) für Bounces und Beschwerden verwendet wird, die der Anbieter (SES) anhand einer Adresse verfolgt, die ihm gehört.
  - Damit DKIM das DMARC-Alignment bestehen kann, muss die in der DKIM-Signatur angegebene Domäne mit der Domäne in der Absenderadresse übereinstimmen. Wenn Sie Absender oder Dienste von Drittanbietern verwenden, die in Ihrem Namen E-Mails versenden, können Sie dies erreichen, indem Sie sicherstellen, dass der Drittanbieter-Absender ordnungsgemäß für die DKIM-Signatur konfiguriert ist und Sie die entsprechenden DNS-Einträge innerhalb Ihrer Domain hinzugefügt haben. Empfangende Mailserver können dann die von Ihrem Drittanbieter an sie gesendeten E-Mails verifizieren, als ob es sich um E-Mails von einer Person handeln würde, die berechtigt ist, eine Adresse innerhalb der Domain zu verwenden.

Alles mit DMARC zusammenfügen

Die oben besprochenen DMARC-Alignment-Checks zeigen, wie SPF, DKIM und DMARC zusammenarbeiten, um das Vertrauen in Ihre Domain und die Zustellung Ihrer E-Mails an

Posteingänge zu erhöhen. DMARC erreicht dies, indem es sicherstellt, dass die Absenderadresse, die der Empfänger sieht, entweder durch SPF oder DKIM authentifiziert wird:

- Eine Nachricht durchläuft DMARC, wenn eine oder beide der beschriebenen SPF- oder DKIM-Prüfungen bestehen.
- Eine Nachricht besteht DMARC nicht, wenn beide der beschriebenen SPF- oder DKIM-Prüfungen fehlschlagen.

Daher sind sowohl SPF als auch DKIM erforderlich, damit DMARC die besten Chancen hat, eine Authentifizierung für Ihre gesendete E-Mail zu erreichen. Wenn Sie alle drei verwenden, tragen Sie dazu bei, dass Sie über eine vollständig geschützte Absenderdomäne verfügen.

Mit DMARC können Sie E-Mail-Servern auch anhand von von Ihnen festgelegter Richtlinien anweisen, wie sie mit E-Mails umgehen sollen, wenn sie die DMARC-Authentifizierung nicht bestehen. Dies wird im folgenden Abschnitt erläutertthe section called “Einrichten der DMARC-Richtlinie für Ihre Domäne”, der Informationen zur Konfiguration Ihrer SES-Domains enthält, sodass die von Ihnen gesendeten E-Mails dem DMARC-Authentifizierungsprotokoll sowohl über SPF als auch über DKIM entsprechen.

Einrichten der DMARC-Richtlinie für Ihre Domäne

Zum Einrichten von DMARC müssen Sie die DNS-Einstellungen für Ihre Domäne ändern. Die DNS-Einstellungen für Ihre Domäne sollten einen TXT-Datensatz enthalten, der die DMARC-Einstellungen der Domäne angibt. Die Verfahren zum Hinzufügen von TXT-Datensätzen zu Ihrer DNS-Konfiguration hängen davon ab, welche DNS- oder Hosting-Anbieter Sie verwenden. Wenn Sie Route 53 verwenden, lesen Sie die Informationen zum Bearbeiten von Datensätzen im Amazon-Route-53-Entwicklerhandbuch. Wenn Sie einen anderen Anbieter verwenden, informieren Sie sich in der Dokumentation zur DNS-Konfiguration des betreffenden Anbieters.

Der Name des von Ihnen erstellten TXT-Datensatzes sollte `_dmarc.`*`example.com`* lauten, wobei *`example.com`* Ihre Domäne ist. Der Wert des TXT-Datensatzes enthält die DMARC-Richtlinie, die auf Ihre Domäne zutrifft. Nachfolgend finden Sie ein Beispiel eines TXT-Datensatzes mit einer DMARC-Richtlinie:

Name	Typ	Wert
`_dmarc.example.com`	`TXT`	`"v=DMARC1;p=quaran tine;rua=mailto:my`

Name	Typ	Wert
		`_dmarc_report@exam ple.com"`

Im vorherigen Beispiel für eine DMARC-Richtlinie weist diese Richtlinie E-Mail-Anbieter an, Folgendes zu tun:

- Senden Sie alle Nachrichten, bei denen die Authentifizierung fehlschlägt, an den Spam-Ordner, `p=quarantine` wie im Richtlinienparameter angegeben. Zu den weiteren Optionen gehört, dass Sie nichts tun`p=none`, indem Sie die Nachricht verwenden, oder die Nachricht direkt zurückweisen. `p=reject`
  - Im nächsten Abschnitt wird erläutert, wie und wann Sie diese drei Richtlinieneinstellungen verwenden sollten. Wenn Sie die falsche Einstellung zur falschen Zeit verwenden, kann dies dazu führen, dass Ihre E-Mail nicht zugestellt wird, siehe. the section called “Implementierung von DMARC”
- Senden Sie Berichte über alle E-Mails, bei denen die Authentifizierung fehlgeschlagen ist, in einem Digest (d. h. einem Bericht, der die Daten für einen bestimmten Zeitraum zusammenfasst, anstatt einzelne Berichte für jedes Ereignis zu senden), wie im Berichtsparameter angegeben `rua=mailto:my_dmarc_report@example.com` (rua steht für Berichts-URI für Aggregierte Berichte). E-Mail-Anbieter senden diese aggregierten Berichten in der Regel einmal pro Tag, wobei diese Richtlinien von Anbieter zu Anbieter verschieden sind.

Weitere Informationen zur Konfiguration von DMARC für Ihre Domäne finden Sie in der Übersicht über die DMARC-Website.

Vollständige Spezifikationen des DMARC-Systems finden Sie unter DMARC-Entwurf der Internet Engineering Task Force (IETF).

Bewährte Methoden für die Implementierung von DMARC

Es ist am besten, die Durchsetzung Ihrer DMARC-Richtlinien schrittweise und schrittweise umzusetzen, damit der Rest Ihres E-Mail-Flusses nicht unterbrochen wird. Erstellen und implementieren Sie einen Rollout-Plan, der diesen Schritten folgt. Führen Sie jeden dieser Schritte zuerst mit jeder Ihrer Subdomänen und schließlich mit der Top-Level-Domain in Ihrer Organisation aus, bevor Sie mit dem nächsten Schritt fortfahren.

1. Überwachen Sie die Auswirkungen der Implementierung von DMARC (p=none).
   - Beginnen Sie mit einem einfachen Datensatz im Überwachungsmodus für eine Subdomain oder Domain, der anfordert, dass E-Mail-Empfangsunternehmen Ihnen Statistiken über Nachrichten senden, die sie unter Verwendung dieser Domain sehen. Ein Datensatz im Überwachungsmodus ist ein DMARC-TXT-Eintrag, dessen Richtlinie auf „Keine“ gesetzt ist. `p=none`
   - Über DMARC generierte Berichte geben die Anzahl und Herkunft der Nachrichten an, die diese Prüfungen bestehen, im Vergleich zu Nachrichten, die dies nicht tun. Sie können leicht erkennen, wie viel Ihres legitimen Datenverkehrs von ihnen abgedeckt wird oder nicht. Sie werden Anzeichen einer Weiterleitung erkennen, da weitergeleitete Nachrichten SPF- und DKIM-Fehler aufweisen, wenn der Inhalt geändert wird. Außerdem werden Sie feststellen, wie viele betrügerische Nachrichten gesendet wurden und von wo sie gesendet wurden.
   - Ziel dieses Schritts ist es, herauszufinden, welche E-Mails betroffen sein werden, wenn Sie einen der nächsten beiden Schritte implementieren, und sicherzustellen, dass alle Drittanbieter oder autorisierten Absender ihre SPF- oder DKIM-Richtlinien aufeinander abstimmen.
   - Am besten für bestehende Domains.
2. Bitten Sie externe E-Mail-Systeme, E-Mails, die DMARC nicht bestehen, unter Quarantäne zu stellen (p=quarantine).
   - Wenn Sie der Meinung sind, dass Ihr gesamter oder der Großteil Ihres legitimen Datenverkehrs domänengerecht entweder SPF oder DKIM versendet wird, und Sie sich der Auswirkungen der Implementierung von DMARC bewusst sind, können Sie eine Quarantänerichtlinie implementieren. Eine Quarantänerichtlinie ist ein DMARC-TXT-Eintrag, dessen Richtlinie auf Quarantäne eingestellt ist. `p=quarantine` Auf diese Weise bitten Sie die DMARC-Empfänger, Nachrichten von Ihrer Domain, die DMARC nicht bestanden haben, in das lokale Äquivalent eines Spam-Ordners zu legen, anstatt in die Posteingänge Ihrer Kunden.
   - Am besten für die Umstellung von Domains, die in Schritt 1 DMARC-Berichte analysiert haben.
3. Fordern Sie an, dass externe Mailsysteme keine Nachrichten akzeptieren, die DMARC nicht bestehen (p=reject).
   - Die Implementierung einer Ablehnungsrichtlinie ist normalerweise der letzte Schritt. Eine Ablehnungsrichtlinie ist ein DMARC-TXT-Eintrag, dessen Richtlinie auf Ablehnung `p=reject` gesetzt ist. Wenn Sie dies tun, bitten Sie die DMARC-Empfänger, keine Nachrichten anzunehmen, die die DMARC-Prüfungen nicht bestehen. Das bedeutet, dass sie nicht einmal in einem Spam- oder Junk-Ordner unter Quarantäne gestellt, sondern sofort abgelehnt werden.

- Wenn Sie eine Ablehnungsrichtlinie verwenden, wissen Sie genau, welche Nachrichten die DMARC-Richtlinie nicht einhalten, da die Ablehnung zu einem SMTP-Bounce führt. Bei Quarantäne liefern die aggregierten Daten Informationen über den Prozentsatz der E-Mails, die SPF-, DKIM- und DMARC-Prüfungen bestanden oder nicht bestanden haben.
- Am besten für neue Domains oder bestehende Domains, die die beiden vorherigen Schritte durchlaufen haben.

Einhaltung von DMARC über SPF

Damit eine E-Mail basierend auf SPF DMARC erfüllt, müssen beide der folgenden Bedingungen erfüllt sein:

- Die Nachricht muss eine SPF-Prüfung bestehen, die auf einem gültigen SPF-Eintrag (Typ TXT) basiert, den Sie in der DNS-Konfiguration Ihrer benutzerdefinierten MAIL FROM-Domäne veröffentlicht haben.
- Die Domain in der Absenderadresse des E-Mail-Headers muss mit der Domain oder einer Subdomain von übereinstimmen, die in der MAIL FROM-Adresse angegeben ist. Um eine SPF-Anpassung an SES zu erreichen, darf die DMARC-Richtlinie der Domain keine strikte SPF-Richtlinie (aspf=s) vorschreiben.

Gehen Sie wie folgt vor, um diese Anforderungen zu erfüllen:

- Befolgen Sie die Anleitung unter the section called “Verwenden einer benutzerdefinierten MAIL FROM-Domäne”, um eine benutzerdefinierte MAIL FROM-Domäne einzurichten.
- Stellen Sie sicher, dass Ihre sendende Domäne eine lockere Richtlinie für SPF verwendet. Wenn Sie die Ausrichtung der Richtlinien Ihrer Domain nicht geändert haben, verwendet sie standardmäßig eine lockere Richtlinie, ebenso wie SES.

> **Note**
>
> Um die DMARC-Ausrichtung Ihrer Domäne für SPF herauszufinden, geben Sie in der Befehlszeile den folgenden Befehl ein. Ersetzen Sie dabei *example.com* durch Ihre Domäne:
>
> ```
> dig TXT _dmarc.example.com
> ```

Suchen Sie in der Ausgabe des Befehls unter Non-authoritative answer nach einem Eintrag, der mit `v=DMARC1` beginnt. Wenn dieser Eintrag die Zeichenfolge `aspf=r` enthält oder die Zeichenfolge `aspf` nicht vorhanden ist, verwendet Ihre Domäne eine lockere Ausrichtung für SPF. Wenn der Eintrag die Zeichenfolge `aspf=s` enthält, verwendet Ihre Domäne eine enge Ausrichtung für SPF. In diesem Fall muss der Systemadministrator diesen Tag in der DNS-Konfiguration Ihrer Domäne aus dem DMARC TXT-Eintrag entfernen.
Alternativ können Sie ein webbasiertes DMARC-Lookup-Tool verwenden, z. B. den DMARC Inspector von der dmarcian-Website oder das DMARC Check Tool-Tool von der MxToolBox Website, um die Richtlinienausrichtung Ihrer Domain für SPF zu ermitteln.

Einhaltung von DMARC über DKIM

Damit eine E-Mail basierend auf DKIM DMARC erfüllt, müssen beide der folgenden Bedingungen erfüllt sein:

- Die Nachricht muss eine gültige DKIM-Signatur haben und die DKIM-Prüfung bestanden haben.
- Die in der DKIM-Signatur angegebene Domäne muss mit der Domäne in der Absenderadresse übereinstimmen (übereinstimmen). Wenn die DMARC-Richtlinie der Domain eine strikte Ausrichtung für DKIM vorsieht, müssen diese Domänen exakt übereinstimmen (SES verwendet standardmäßig eine strikte DKIM-Richtlinie).

Gehen Sie wie folgt vor, um diese Anforderungen zu erfüllen:

- Richten Sie Easy DKIM anhand der Anleitung unter the section called “Easy DKIM” ein. Wenn Sie Easy DKIM verwenden, signiert Amazon SES Ihre E-Mails automatisch.

> **Note**
>
> Statt Easy DKIM zu verwenden, können Sie Ihre Nachrichten auch manuell signieren. Diese Methode ist jedoch mit Vorsicht zu verwenden, da Amazon SES die von Ihnen erstellte DKIM-Signatur nicht validiert. Daher empfehlen wir dringend die Verwendung von Easy DKIM.

- Stellen Sie sicher, dass die in der DKIM-Signatur angegebene Domain mit der Domain in der Absenderadresse übereinstimmt. Oder, wenn Sie von einer Subdomain der Domain in der

Absenderadresse senden, stellen Sie sicher, dass Ihre DMARC-Richtlinie auf eine lockere Ausrichtung eingestellt ist.

> **Note**
>
> Um die DMARC-Ausrichtung Ihrer Domäne für DKIM herauszufinden, geben Sie in der Befehlszeile den folgenden Befehl ein. Ersetzen Sie dabei *example.com* durch Ihre Domäne:
>
> ```
> dig TXT _dmarc.example.com
> ```
>
> Suchen Sie in der Ausgabe des Befehls unter Non-authoritative answer nach einem Eintrag, der mit `v=DMARC1` beginnt. Wenn dieser Eintrag die Zeichenfolge `adkim=r` enthält oder die Zeichenfolge `adkim` nicht vorhanden ist, verwendet Ihre Domäne eine lockere Ausrichtung für DKIM. Wenn der Eintrag die Zeichenfolge `adkim=s` enthält, verwendet Ihre Domäne eine enge Ausrichtung für DKIM. In diesem Fall muss der Systemadministrator diesen Tag in der DNS-Konfiguration Ihrer Domäne aus dem DMARC TXT-Eintrag entfernen.
> Alternativ können Sie ein webbasiertes DMARC-Lookup-Tool verwenden, z. B. den DMARC Inspector von der dmarcian-Website oder das DMARC Check Tool-Tool von der MxToolBox Website, um die Richtlinienausrichtung Ihrer Domain für DKIM zu ermitteln.

Verwenden von BIMI in Amazon SES

Brand Indicators for Message Identification (BIMI) ist eine E-Mail-Spezifikation, mit der in E-Mail-Posteingängen das Logo einer Marke neben den authentifizierten E-Mail-Nachrichten der Marke in unterstützenden E-Mail-Clients angezeigt werden kann.

BIMI ist eine E-Mail-Spezifikation, die direkt mit der Authentifizierung verbunden ist. Es handelt sich jedoch nicht um ein eigenständiges E-Mail-Authentifizierungsprotokoll, da alle Ihre E-Mails der DMARC-Authentifizierung entsprechen müssen.

BIMI erfordert zwar DMARC, DMARC erfordert jedoch, dass Ihre Domain entweder SPF- oder DKIM-Einträge zum Abgleichen hat. Es ist jedoch am besten, sowohl SPF- als auch DKIM-Einträge hinzuzufügen, um zusätzliche Sicherheit zu gewährleisten und weil einige E-Mail-Dienstanbieter () ESPs beide benötigen, wenn sie BIMI verwenden. Im folgenden Abschnitt werden die Schritte zur Implementierung von BIMI in Amazon SES beschrieben.

Einrichtung von BIMI in SES

Sie können BIMI für eine E-Mail-Domain konfigurieren, die Sie besitzen – in SES wird dies als benutzerdefinierte MAIL FROM-Domain bezeichnet. Nach der Konfiguration wird in allen Nachrichten, die Sie von dieser Domain senden, Ihr BIMI-Logo in E-Mail-Clients angezeigt, die BIMI unterstützen.

Damit Ihre E-Mails ein BIMI-Logo anzeigen können, müssen innerhalb von SES einige Voraussetzungen erfüllt sein. Im folgenden Verfahren werden diese Voraussetzungen verallgemeinert und es wird auf spezielle Abschnitte verwiesen, die diese Themen ausführlich behandeln. Die für BIMI spezifischen Schritte und die für die Konfiguration in SES erforderliche Vorgehensweise werden hier ausführlich beschrieben.

So richten Sie eine benutzerdefinierte MAIL FROM-Domain ein

1. Sie müssen eine benutzerdefinierte MAIL FROM-Domain in SES konfiguriert haben, in der sowohl SPF- (Typ TXT) als auch MX-Einträge für diese Domain veröffentlicht sind. Wenn Sie keine benutzerdefinierte MAIL FROM-Domain haben oder eine neue für Ihr BIMI-Logo erstellen möchten, finden Sie weitere Informationen unter the section called “Verwenden einer benutzerdefinierten MAIL FROM-Domäne”.
2. Konfigurieren Sie Ihre Domain mit Easy DKIM. Siehe the section called “Easy DKIM”.
3. Konfigurieren Sie Ihre Domain mit DMARC, indem Sie bei Ihrem DNS-Anbieter einen TXT-Eintrag veröffentlichen, der die folgenden für BIMI erforderlichen Durchsetzungsrichtlinien enthält, die einem der beiden Beispiele ähneln:

Name	Typ	Wert
`_dmarc.example.com`	`TXT`	`v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarcreports@example.com`
`_dmarc.example.com`	`TXT`	`v=DMARC1;p=reject;rua=mailto:dmarcreports@example.com`

Im vorherigen Beispiel für eine DMARC-Richtlinie, wie für BIMI erforderlich:

- *`example.com`* sollte durch Ihren Domain- oder Subdomainnamen ersetzt werden.
- Der Wert p= kann einer der folgenden sein:

    - Quarantäne mit einem PCT-Wert, der wie abgebildet auf 100 festgelegt ist, oder
    - ablehnen wie gezeigt.
  - Wenn Sie von einer Subdomain aus senden, ist für BIMI erforderlich, dass die übergeordnete Domain ebenfalls über diese Durchsetzungsrichtlinie verfügen muss. Subdomains fallen unter die Richtlinie der übergeordneten Domain. Wenn Sie jedoch zusätzlich zu dem, was für die übergeordnete Domain veröffentlicht wird, einen DMARC-Eintrag für Ihre Subdomain hinzufügen, muss Ihre Subdomain ebenfalls über dieselbe Durchsetzungsrichtlinie verfügen, um für BIMI infrage zu kommen.
  - Wenn Sie noch nie eine DMARC-Richtlinie für Ihre Domain eingerichtet haben, lesen Sie den Abschnitt the section called “Authentifizierung Ihrer E-Mails mit DMARC” und stellen Sie sicher, dass Sie nur die DMARC-Richtlinienwerte verwenden, die für BIMI spezifisch sind, wie abgebildet.
4. Produzieren Sie Ihr BIMI-Logo als `.svg` SVG-Datei (Scalable Vector Graphics) — das spezifische SVG-Profil, das von BIMI benötigt wird, ist als SVG (SVG P/S) definiert. Portable/Secure Damit Ihr Logo im E-Mail-Client angezeigt werden kann, muss es genau diesen Spezifikationen entsprechen. Lesen Sie die Anleitung der BIMI Group zur Erstellung von SVG-Logodateien und zu den empfohlenen SVG-Konvertierungstools.
5. (Optional) Besorgen Sie sich ein Verified Mark Certificate (VMC). Einige ESPs, wie Gmail und Apple, verlangen eine VMC, um nachzuweisen, dass Sie die Marke und den Inhalt Ihres BIMI-Logos besitzen. Dies ist zwar keine Voraussetzung für die Implementierung von BIMI in Ihrer Domain, Ihr BIMI-Logo wird jedoch nicht im E-Mail-Client angezeigt, wenn der ESP, an den Sie E-Mails senden, die VMC-Compliance erzwingt. Sehen Sie sich die Verweise der BIMI Group auf die teilnehmenden Zertifizierungsstellen an, um ein VMC für Ihr Logo zu erhalten.
6. Hosten Sie die SVG-Datei Ihres BIMI-Logos auf einem Server, auf den Sie Zugriff haben, um sie über HTTPS öffentlich zugänglich zu machen. Sie könnten sie beispielsweise in einen Amazon-S3-Bucket hochladen.
7. Erstellen und veröffentlichen Sie einen BIMI-DNS-Eintrag, der eine URL zu Ihrem Logo enthält. Wenn ein ESP, der BIMI unterstützt, Ihren DMARC-Eintrag überprüft, sucht er auch nach einem BIMI-Datensatz, der die URL für die `.svg`-Datei Ihres Logos und, falls konfiguriert, die URL für die `.pem`-Datei Ihres VMC enthält. Wenn die Einträge übereinstimmen, wird Ihr BIMI-Logo angezeigt.

   Konfigurieren Sie Ihre Domain mit BIMI, indem Sie einen TXT-Eintrag mit Ihrem DNS-Anbieter mit den folgenden Werten wie gezeigt veröffentlichen. Das Senden von einer Domain wird im ersten Beispiel und das Senden von einer Subdomain im zweiten Beispiel dargestellt:

Name	Typ	Wert
`default._bimi.example.com`	TXT	`v=BIMI1;l=https://myhostingserver.com/images/logo.svg;a=https://myhostingserver.com/certificate/vmc_2023-01-01.pem`
`default._bimi.marketing.example.com`		

In den vorhergehenden BIMI-Eintragsbeispielen:

- Der Namenswert sollte wörtlich `default._bimi.` als Subdomain von *`example.com`* oder *`marketing.example.com`* angeben, was durch Ihren Domain- oder Subdomainnamen ersetzt werden sollte.
- Der Wert `v=` ist die Version des BIMI-Eintrags.
- Der Wert `l=` ist das Logo, das die URL darstellt, die auf die `.svg`-Datei Ihres Image verweist.
- Der Wert `a=` ist die Zertifizierungsstelle, die die URL darstellt, die auf die `.pem`-Datei Ihres Zertifikats verweist.

Sie können Ihren BIMI-Eintrag mit einem Tool wie BIMI Inspector der BIMI Group validieren.

Der letzte Schritt in diesem Prozess besteht darin, ein regelmäßiges Sendemuster an diejenigen zu haben ESPs , die die Platzierung des BIMI-Logos unterstützen. Ihre Domain sollte einen regelmäßigen Zustellrhythmus haben und bei der Domain, an die Sie senden ESPs , einen guten Ruf haben. Es kann einige Zeit dauern, bis die Platzierung des BIMI-Logos so weit verbreitet ist ESPs , dass Sie keinen guten Ruf oder keine Versandfrequenz haben.

Weitere Informationen und Ressourcen zu BIMI finden Sie über BIMI Group.

Einrichten von Ereignisbenachrichtigungen für Amazon SES

Um E-Mails mit Amazon SES zu senden, müssen Sie ein System für die Verwaltung von Unzustellbarkeitsnachrichten und Beschwerden haben. Amazon SES kann Sie auf drei Arten über Unzustellbarkeits- und Beschwerdeereignisse informieren: durch Senden einer Benachrichtigungs-E-Mail, durch Benachrichtigung eines Amazon-SNS-Themas oder durch Veröffentlichung von Sendeereignissen. Dieser Abschnitt enthält Informationen über das Einrichten von Amazon SES

zum Senden bestimmter Arten von Benachrichtigungen per E-Mail oder durch Benachrichtigen eines Amazon-SNS-Themas. Weitere Informationen zum Veröffentlichen von Sendeereignissen finden Sie unter Überwachen des E-Mail-Versands mithilfe der Amazon SES-Ereignisveröffentlichung.

Sie können Benachrichtigungen mithilfe der Amazon-SES-Konsole oder der Amazon-SES-API einrichten.

Themen

- Wichtige Überlegungen
- Verwenden von Benachrichtigungen für den Amazon-SES-E-Mail-Empfang
- Verwenden von Benachrichtigungen für den Amazon SNS E-Mail-Empfang

Wichtige Überlegungen

Es sind mehrere wichtige Punkte zu berücksichtigen, wenn Sie Amazon SES zum Senden von Benachrichtigungen einrichten:

- E-Mail- und Amazon-SNS-Benachrichtigungen gelten für einzelne Identitäten (die verifizierten E-Mail-Adressen oder Domänen, die Sie zum Senden von E-Mails verwenden). Wenn Sie Benachrichtigungen für eine Identität aktivieren, sendet Amazon SES nur Benachrichtigungen für E-Mails, die von dieser Identität gesendet wurden, und zwar nur in der AWS Region, in der Sie Benachrichtigungen konfiguriert haben.
- Sie müssen eine Methode für den Empfang von Unzustellbarkeits- und Beschwerdebenachrichtigungen aktivieren. Sie können Benachrichtigungen an die Domäne oder E-Mail-Adresse senden, die die unzustellbare E-Mail und Beschwerde generiert hat, oder an ein Amazon-SNS-Thema. Sie können das Veröffentlichen von Veranstaltungen auch verwenden, um Benachrichtigungen über verschiedene Arten von Ereignissen (einschließlich Bounces, Beschwerden, Lieferungen und mehr) an ein Amazon SNS SNS-Thema oder einen Firehose-Stream zu senden.

  Wenn Sie keine dieser Methoden für den Empfang von Unzustellbarkeits- oder Beschwerdebenachrichtigungen einrichten, leitet Amazon SES Unzustellbarkeits- und Beschwerdebenachrichtigungen automatisch weiter an die „Return-Path“-Adresse (Antwortpfad bei Unzustellbarkeit) (oder die „Source“-Adresse (Quelle), wenn Sie keine "Return-Path"-Adresse angegeben haben) in der E-Mail, die das Unzustellbarkeits- und Beschwerdeereignis ausgelöst hat, selbst wenn Sie die Weiterleitung von E-Mail-Feedback deaktiviert haben.

Wenn Sie die Weiterleitung von E-Mail-Feedback deaktivieren und Ereignisveröffentlichung aktivieren, müssen Sie den Konfigurationssatz, der die Ereignisveröffentlichungsregel enthält, auf alle E-Mails, die Sie senden, anwenden. In diesem Fall, wenn Sie den Konfigurationssatz nicht verwenden, leitet Amazon SES Unzustellbarkeits- und Beschwerdebenachrichtigungen automatisch weiter an die „Return-Path“-Adresse (Antwortpfad bei Unzustellbarkeit) oder die „Source“-Adresse (Quelle) in der E-Mail, die das Unzustellbarkeits- und Beschwerdeereignis ausgelöst hat.

- Wenn Sie Amazon SES für das Senden von Unzustellbarkeits- und Beschwerdeereignissen mithilfe von mehr als einer Methode einrichten (z. B. durch das Senden von E-Mail-Benachrichtigungen und durch das Senden von Ereignissen), erhalten Sie möglicherweise mehr als eine Benachrichtigung für dasselbe Ereignis.

Verwenden von Benachrichtigungen für den Amazon-SES-E-Mail-Empfang

Amazon SES kann Ihnen eine E-Mail senden, wenn Sie Unzustellbarkeitsnachrichten und Beschwerden erhalten, indem ein Prozess namens Weiterleitung von E-Mail-Feedback angewandt wird.

Zum Senden von E-Mails mit Amazon SES müssen Sie es so konfigurieren, dass Unzustellbarkeits- und Beschwerdebenachrichtigungen gesendet werden. Verwenden Sie dazu eine der folgenden Methoden:

- Aktivieren der Weiterleitung von E-Mail-Feedback. Die Schritte zum Einrichten dieser Art von Benachrichtigung sind in diesem Abschnitt enthalten.
- Senden von Benachrichtigungen an ein Amazon-SNS-Thema. Weitere Informationen finden Sie unter Verwenden von Benachrichtigungen für den Amazon SNS E-Mail-Empfang.
- Veröffentlichen von Ereignisbenachrichtigungen. Weitere Informationen finden Sie unter Überwachen des E-Mail-Versands mithilfe der Amazon SES-Ereignisveröffentlichung.

> **Important**
>
> Wichtige Informationen zu Benachrichtigungen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.

Themen

- Aktivieren der E-Mail-Feedback-Weiterleitung
- Deaktivieren der E-Mail-Feedback-Weiterleitung
- E-Mail-Feedback-Weiterleitungsziel

Aktivieren der E-Mail-Feedback-Weiterleitung

Die E-Mail-Feedback-Weiterleitung ist standardmäßig aktiviert. Wenn Sie sie zuvor deaktiviert haben, können Sie sie mit der folgenden Vorgehensweise in diesem Abschnitt aktivieren.

So ermöglichen Sie die Weiterleitung von Unzustellbarkeits- und Beschwerdebenachrichtigungen per E-Mail über die Amazon-SES-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der verifizierten E-Mail-Adressen oder Domänen die E-Mail-Adresse oder Domäne aus, für die Sie Unzustellbarkeits- und Beschwerdebenachrichtigungen konfigurieren möchten.
4. Erweitern Sie im Detailbereich den Abschnitt Notifications (Benachrichtigungen).
5. Wählen Sie Edit Configuration (Konfiguration bearbeiten) aus.
6. Wählen Sie unter Email Feedback Forwarding (E-Mail-Feedback-Weiterleitung) die Option Enabled (Aktiviert) aus.

> **Note**
>
> Bis Änderungen, die Sie auf dieser Seite vornehmen, wirksam werden, können einige Minuten vergehen.

Mithilfe der SetIdentityFeedbackForwardingEnabledAPI-Operation können Sie auch Benachrichtigungen über Rücksendungen und Beschwerden per E-Mail aktivieren.

Deaktivieren der E-Mail-Feedback-Weiterleitung

Wenn Sie eine andere Methode zur Bereitstellung von Unzustellbarkeits- und Beschwerdebenachrichtigungen einrichten, können Sie die Weiterleitung von E-Mail-Feedback

deaktivieren, sodass Sie nicht mehrere Benachrichtigungen erhalten, wenn ein Unzustellbarkeits- und Beschwerdeereignis eintritt.

So deaktivieren Sie die Weiterleitung von Unzustellbarkeits- und Beschwerdebenachrichtigungen per E-Mail über die Amazon-SES-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der verifizierten E-Mail-Adressen oder Domänen die E-Mail-Adresse oder Domäne aus, für die Sie Unzustellbarkeits- und Beschwerdebenachrichtigungen konfigurieren möchten.
4. Erweitern Sie im Detailbereich den Abschnitt Notifications (Benachrichtigungen).
5. Wählen Sie Edit Configuration (Konfiguration bearbeiten) aus.
6. Wählen Sie unter Email Feedback Forwarding (E-Mail-Feedback-Weiterleitung) die Option Disabled (Deaktiviert) aus.

> **Note**
>
> Sie müssen eine Methode für den Empfang von Unzustellbarkeits- und Beschwerdebenachrichtigungen konfigurieren, um E-Mails über Amazon SES senden zu können. Wenn Sie die Weiterleitung von Feedback per E-Mail deaktivieren, müssen Sie die von Amazon SNS gesendeten Benachrichtigungen aktivieren oder Bounce- und Beschwerdeereignisse mithilfe von Event Publishing in einem Amazon SNS SNS-Thema oder einem Firehose-Stream veröffentlichen. Wenn Sie Ereignisveröffentlichung verwenden, müssen Sie auch den Konfigurationssatz, der die Ereignisveröffentlichungsregel enthält, auf jede E-Mail, die Sie senden, anwenden. Wenn Sie keine Methode für den Empfang von Unzustellbarkeits- und Beschwerdebenachrichtigungen einrichten, leitet Amazon SES Feedback-Benachrichtigungen automatisch per E-Mail weiter an die Adresse im Feld „Return-Path“ (Antwortpfad bei Unzustellbarkeit) (oder im Feld „Source“ (Quelle), wenn Sie keine „Return-Path“-Adresse angegeben haben) der Nachricht, die das Unzustellbarkeits- und Beschwerdeereignis ausgelöst hat. In diesem Fall leitet Amazon SES Unzustellbarkeits- und Beschwerdebenachrichtigungen weiter, auch wenn Sie Benachrichtigungen über E-Mail-Feedback deaktiviert haben.

7. Wählen Sie Save Config, um die Benachrichtigungskonfiguration zu speichern.

> **Note**
>
> Bis Änderungen, die Sie auf dieser Seite vornehmen, wirksam werden, können einige Minuten vergehen.

Mithilfe der API-Operation können Sie auch Benachrichtigungen über Bounce und Beschwerden per E-Mail deaktivieren. SetIdentityFeedbackForwardingEnabled

E-Mail-Feedback-Weiterleitungsziel

Wenn Sie Benachrichtigungen per E-Mail erhalten, schreibt Amazon SES die `From` Kopfzeile neu und sendet die Benachrichtigung an Sie. Die Adresse, an die Amazon SES die Benachrichtigung weiterleitet, hängt davon ab, wie Sie die Originalnachricht versendet haben.

Wenn Sie die Nachricht über die SMTP-Schnittstelle versendet haben, werden die Benachrichtigungen entsprechend den folgenden Regeln zugestellt:

- Wenn Sie im `SMTP DATA`-Abschnitt eine `Return-Path`-Kopfzeile angegeben haben, werden die Benachrichtigungen an diese Adresse gesendet.
- Andernfalls werden Benachrichtigungen an die Adresse gesendet, die Sie bei der Eingabe des Befehls MAIL FROM angegeben haben.

Wenn Sie die Nachricht über die `SendEmail`-API-Operation versendet haben, werden die Benachrichtigungen entsprechend den folgenden Regeln zugestellt:

- Wenn Sie im Aufruf der `SendEmail`-API den optionalen `ReturnPath`-Parameter angegeben haben, dann werden Benachrichtigungen an diese Adresse gesendet.
- Andernfalls werden Benachrichtigungen an die Adresse gesendet, die im erforderlichen `Source`-Parameter von `SendEmail` angegeben wird.

Wenn Sie die Nachricht über die `SendRawEmail`-API-Operation versendet haben, werden die Benachrichtigungen entsprechend den folgenden Regeln zugestellt:

- Wenn Sie in der unformatierten Nachricht eine `Return-Path`-Kopfzeile angegeben haben, werden die Benachrichtigungen an diese Adresse gesendet.

- Wenn Sie im Aufruf der `SendRawEmail`-API einen `Source`-Parameter angegeben haben, werden Benachrichtigungen andernfalls an diese Adresse gesendet.
- Andernfalls werden Benachrichtigungen an die Adresse in der Kopfzeile `From` der unformatierten Nachricht gesendet.

> **Note**
>
> Wenn Sie eine `Return-Path`-Adresse in einer E-Mail angeben, erhalten Sie Benachrichtigungen an dieser Adresse. Die Version der Nachricht, die der Empfänger erhält, enthält jedoch eine `Return-Path`-Kopfzeile mit einer anonymisierten E-Mail-Adresse (z. B. a0b1c2d3e4f5a6b7-c8d9e0f1-a2b3-c4d5-e6f7-a8b9c0d1e2f3-000000@amazonses.com). Diese Anonymisierung findet unabhängig davon statt, wie Sie die E-Mail gesendet haben.

Verwenden von Benachrichtigungen für den Amazon SNS E-Mail-Empfang

Sie können Amazon SES so konfigurieren, dass ein Amazon-SNS-Thema benachrichtigt wird, wenn Sie Unzustellbarkeitsnachrichten oder Beschwerden erhalten oder wenn E-Mails übermittelt werden. Amazon SNS SNS-Benachrichtigungen sind im Format JavaScript Object Notation (JSON), sodass Sie sie programmgesteuert verarbeiten können.

Zum Senden von E-Mails mit Amazon SES müssen Sie es so konfigurieren, dass Unzustellbarkeits- und Beschwerdebenachrichtigungen gesendet werden. Verwenden Sie dazu eine der folgenden Methoden:

- Senden von Benachrichtigungen an ein Amazon-SNS-Thema. Die Schritte zum Einrichten dieser Art von Benachrichtigung sind in diesem Abschnitt enthalten.
- Aktivieren der Weiterleitung von E-Mail-Feedback. Weitere Informationen finden Sie unter Verwenden von Benachrichtigungen für den Amazon-SES-E-Mail-Empfang.
- Veröffentlichen von Ereignisbenachrichtigungen. Weitere Informationen finden Sie unter Überwachen des E-Mail-Versands mithilfe der Amazon SES-Ereignisveröffentlichung.

> **Important**
>
> Wichtige Informationen zu Benachrichtigungen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.

Themen

- Konfigurieren von Amazon-SNS-Benachrichtigungen für Amazon SES
- Amazon-SNS-Benachrichtigungsinhalte für Amazon SES
- Amazon-SNS-Benachrichtigungsbeispiele für Amazon SES

Konfigurieren von Amazon-SNS-Benachrichtigungen für Amazon SES

Amazon SES kann Sie über Unzustellungszustellungen, Beschwerden und Zustellungen überAmazon Simple Notification Service (Amazon SNS)benachrichtigen.

Sie können die Benachrichtigungen mit der Amazon-SES-Konsole oder mithilfe der Amazon-SES-API konfigurieren.

Themen in diesem Abschnitt:

- Voraussetzungen
- Konfigurieren von Benachrichtigungen mit der Amazon-SES-Konsole
- Konfigurieren von Benachrichtigungen mit der Amazon-SES-API
- Fehlerbehebung bei Feedback-Benachrichtigungen

Voraussetzungen

Führen Sie die folgenden Schritte aus, bevor Sie Amazon-SNS-Benachrichtigungen in Amazon SES einrichten:

1. Erstellen Sie ein Amazon SNS-Thema. Weitere Informationen finden Sie unter Erstellen eines Themas im Amazon Simple Notification Service-Entwicklerhandbuch.

   > **Important**
   >
   > Wenn Sie Ihr Thema mit Amazon SNS erstellen, wählen Sie für Type (Typ) nur Standard (Standard) aus. (SES unterstützt keine FIFO-Typ-Themen.)

   Unabhängig davon, ob Sie ein neues SNS-Thema erstellen oder ein vorhandenes auswählen, müssen Sie Zugriff auf SES gewähren, um Benachrichtigungen für das Thema zu veröffentlichen.

Um Amazon SES die Berechtigung zum Veröffentlichen von Benachrichtigungen für das Thema zu erteilen, erweitern Sie auf dem Bildschirm Edit topic (Thema bearbeiten) der SNS-Konsole die Access policy (Zugriffsrichtlinie) und fügen Sie im JSON editor (JSON-Editor) die folgende Berechtigungsrichtlinie hinzu:

JSON

```
{
    "Version":"2012-10-17",
    "Id": "notification-policy",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "sns:Publish",
            "Resource": "arn:aws:sns:us-east-1:111122223333:topic_name",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "111122223333",
                    "AWS:SourceArn":
 "arn:aws:ses:topic_region:111122223333:identity/identity_name"
                }
            }
        }
    ]
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- *topic_region*Ersetzen Sie es durch die AWS Region, in der Sie das SNS-Thema erstellt haben.
- Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID.
- *topic_name*Ersetzen Sie es durch den Namen Ihres SNS-Themas.
- Ersetze es durch die verifizierte Identität (E-Mail-Adresse oder Domain), *identity_name* mit der du das SNS-Thema abonniert hast.

2. Abonnieren Sie mindestens einen Endpunkt für das Thema. Wenn Sie beispielsweise Benachrichtigungen per Textnachricht erhalten möchten, abonnieren Sie einen SMS-Endpunkt (d. h. eine Mobiltelefonnummer) für das Thema. Um Benachrichtigungen per E-Mail zu erhalten, abonnieren Sie einen E-Mail-Endpunkt (eine E-Mail-Adresse) für das Thema.

   Weitere Informationen dazu erhalten Sie unter Erste Schritte im Amazon Simple Notification Service Leitfaden.

3. (Optional) Wenn Ihr Amazon SNS SNS-Thema AWS Key Management Service (AWS KMS) für die serverseitige Verschlüsselung verwendet, müssen Sie der AWS KMS Schlüsselrichtlinie Berechtigungen hinzufügen. Sie können Berechtigungen hinzufügen, indem Sie die folgende Richtlinie an die Schlüsselrichtlinie anhängen: AWS KMS

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESToUseKMSKey",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Konfigurieren von Benachrichtigungen mit der Amazon-SES-Konsole

So konfigurieren Sie Benachrichtigungen mithilfe der Amazon-SES-Konsole

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.

3. Wählen Sie im Container Identities (Identitäten) die bestätigte Identität aus, für die Sie Feedback-Benachrichtigungen erhalten möchten, wenn eine von dieser Identität gesendete Nachricht entweder zu einer Unzustellbarkeit, Beschwerde oder Zustellung führt.

> **Important**
>
> Die Benachrichtigungseinstellungen für die verifizierte Domäne gelten für alle E-Mail-Adressen in dieser Domäne, außer für E-Mail-Adressen, die auch noch verifiziert sind.

4. Wählen Sie im Detailfenster der ausgewählten bestätigten Identität die Registerkarte Notification (Benachrichtigungen) und wählen Sie Edit (Bearbeiten) im Container Feedback notifications (Feedback-Benachrichtigungen).
5. Erweitern Sie das Listenfeld SNS-Thema jedes Feedback-Typs, für den Sie Benachrichtigungen erhalten möchten, und wählen Sie entweder ein SNS-Thema aus, das Ihnen gehört, No SNS topic (Kein SNS-Thema) oder ein SNS topic you don‘t own (SNS-Thema, das Ihnen nicht gehört).

   - Wenn Sie ein SNS-Thema, das Ihnen nicht gehört, ausgewählt haben, wird das Feld SNS topic ARN (SNS-Themen-ARN) angezeigt, in das Sie den SNS-Themen-ARN eingeben müssen, der Ihnen von Ihrem delegierten Sender mitgeteilt wurde. (Nur Ihr delegierter Sender erhält diese Benachrichtigungen, da er das SNS-Thema besitzt. Weitere Informationen zur Sendung finden Sie unter Übersicht über die Sendeautorisierung.)

> **Important**
>
> Die Amazon SNS SNS-Themen, die Sie für Bounce-, Beschwerde- und Lieferbenachrichtigungen verwenden, müssen dieselben sein AWS-Region , in denen Sie Amazon SES verwenden.
> Zusätzlich müssen Sie einen oder mehrere Endpunkte für das Thema abonniert haben, um Benachrichtigungen zu erhalten. Beispiel: Wenn Sie möchten, dass Benachrichtigungen an eine E-Mail-Adresse gesendet werden, müssen Sie einen E-Mail-Endpunkt für das Thema abonnieren. Weitere Informationen dazu erhalten Sie unter Erste Schritte im Amazon Simple Notification Service Leitfaden.

6. (Optional) Wenn Sie möchten, dass Ihre Themenachrichtigung die Header der ursprünglichen E-Mail einschließt, aktivieren Sie das Kontrollkästchen Include original email headers (Ursprüngliche E-Mail-Header einschließen) direkt unter dem SNS-Themennamen

jedes Feedback-Typs. Diese Option ist nur verfügbar, sofern Sie der zugeordneten Benachrichtigungsart ein Amazon-SNS-Thema zugewiesen haben. Weitere Informationen zum Inhalt der ursprünglichen E-Mail-Header finden Sie im Abschnitt zum `mail`-Objekt unter Benachrichtigungsinhalte.

7. Wählen Sie Änderungen speichern aus. Es kann ein paar Minuten dauern, bis die Änderungen an den Benachrichtigungseinstellungen übernommen werden.
8. (Optional) Wenn Sie Amazon-SNS-Themenbenachrichtigungen sowohl für Unzustellbarkeit als auch für Beschwerden ausgewählt haben, können Sie die E-Mail-Benachrichtigungen vollständig deaktivieren, sodass Sie keine doppelten Benachrichtigungen per E-Mail und SNS-Benachrichtigungen erhalten. Um E-Mail-Benachrichtigungen für Unzustellbarkeiten und Beschwerden zu deaktivieren, wählen Sie auf der Registerkarte Notifications (Benachrichtigungen) auf dem Detailfenster der bestätigten Identität im Container E-Mail-Feedback-Weiterleitung Edit (Bearbeiten), deaktivieren Sie das Kontrollkästchen Enabled (Aktiviert) und wählen Sie Save changes (Änderungen speichern).

Nachdem Sie Ihre Einstellungen konfiguriert haben, werden die Unzustellbarkeits-, Beschwerde- und Zustellungsbenachrichtigungen an Ihre Amazon-SNS-Themen gesendet. Diese Benachrichtigungen sind im Format JavaScript Object Notation (JSON) und folgen der unter beschriebenen Struktur. Benachrichtigungsinhalte

Für Unzustellbarkeits-, Beschwerde- und Zustellungsbenachrichtigungen werden die Amazon-SNS-Standardgebühren erhoben. Weitere Informationen finden Sie in der Amazon-SNS-Preisliste.

> **Note**
>
> Wenn ein Versuch, in Ihrem Amazon SNS SNS-Thema zu veröffentlichen, fehlschlägt, weil das Thema gelöscht wurde oder Sie nicht AWS-Konto mehr über die erforderlichen Berechtigungen verfügen, entfernt Amazon SES die Konfiguration für dieses Thema, sofern es für Bounces oder Beschwerden (nicht für Lieferungen — bei Lieferbenachrichtigungen löscht SES die Konfigurationseinstellung für das SNS-Thema nicht) konfiguriert wurde. Darüber hinaus aktiviert Amazon SES E-Mail-Benachrichtigungen über Unzustellbarkeiten und Beschwerden für die Identität erneut und Sie erhalten per E-Mail eine Benachrichtigung über die Änderung. Wenn mehrere Identitäten für die Verwendung des Themas konfiguriert sind, wird die Themenkonfiguration für jede Identität geändert, wenn bei jeder Identität ein Fehler beim Veröffentlichen des Themas auftritt.

Konfigurieren von Benachrichtigungen mit der Amazon-SES-API

Sie können Unzustellbarkeits-, Beschwerde- und Zustellungsbenachrichtigungen auch mithilfe der Amazon-SES-API konfigurieren. Verwenden Sie zum Konfigurieren von Benachrichtigungen die folgenden Operationen:

- SetIdentityNotificationTopic
- SetIdentityFeedbackForwardingEnabled
- GetIdentityNotificationAttributes
- SetIdentityHeadersInNotificationsEnabled

Sie können mit diesen API-Aktionen eine benutzerdefinierte Front-End-Anwendung für Benachrichtigungen schreiben. Eine vollständige Beschreibung der API-Aktionen für Benachrichtigungen finden Sie in der API-Referenz von Amazon Simple Email Service.

Fehlerbehebung bei Feedback-Benachrichtigungen

Benachrichtigungen werden nicht empfangen

Wenn Sie keine Benachrichtigungen erhalten, stellen Sie sicher, dass Sie einen Endpunkt für das Thema abonniert haben, über das die Benachrichtigungen gesendet werden. Wenn Sie einen E-Mail-Endpunkt für ein Thema abonnieren, erhalten Sie eine E-Mail, in der Sie aufgefordert werden, Ihr Abonnement zu bestätigen. Sie müssen Ihr Abonnement bestätigen, bevor Sie E-Mail-Benachrichtigungen empfangen. Weitere Informationen dazu erhalten Sie unter Erste Schritte im Amazon Simple Notification Service Leitfaden.

`InvalidParameterValue`-Fehler beim Auswählen eines Themas

Wenn Sie eine Fehlermeldung erhalten, die besagt, dass ein `InvalidParameterValue`Fehler aufgetreten ist, überprüfen Sie das Amazon-SNS-Thema, um zu sehen, ob es mit AWS KMS verschlüsselt ist. Ist dies der Fall, müssen Sie die Richtlinie für den Schlüssel ändern. AWS KMS Eine Beispielrichtlinie finden Sie unter Voraussetzungen.

Amazon-SNS-Benachrichtigungsinhalte für Amazon SES

Bounce-, Beschwerde- und Lieferbenachrichtigungen werden unter Amazon Simple Notification Service (Amazon SNS) -Themen im Format JavaScript Object Notation (JSON) veröffentlicht. Das JSON-Objekt der obersten Ebene enthält eine `notificationType`-Zeichenfolge und ein `mail`-Objekt sowie entweder ein `bounce`-Objekt, ein `complaint`-Objekt oder ein `delivery`-Objekt.

In den folgenden Abschnitten finden Sie Beschreibungen der verschiedenen Objekttypen:

- JSON-Objekt der obersten Ebene
- `mail`-Objekt
- `bounce`-Objekt
- `complaint`-Objekt
- `delivery`-Objekt

Im Folgenden finden Sie einige wichtige Hinweise zum Inhalt der Amazon-SNS-Benachrichtigungen für Amazon SES::

- Bei einem angegebenen Benachrichtigungstyp erhalten Sie unter Umständen eine Amazon-SNS-Benachrichtigung für mehrere Empfänger oder aber pro Empfänger eine Amazon-SNS-Benachrichtigung. Ihr Code sollte in der Lage sein, die Amazon SNS-Benachrichtigung zu analysieren und beide Fälle zu behandeln. SES gibt keine Bestell- oder Batching-Garantien für Benachrichtigungen, die über Amazon SNS gesendet werden. Unterschiedliche Amazon-SNS-Benachrichtigungstypen (beispielsweise Unzustellbarkeit und Beschwerden) werden jedoch nicht in einer einzelnen Benachrichtigung zusammengefasst.
- Sie erhalten möglicherweise verschiedene Amazon-SNS-Benachrichtigungstypen für einen Empfänger. So ist es beispielsweise möglich, dass der empfangende E-Mail-Server die E-Mail akzeptiert (und eine Zustellbenachrichtigung auslöst), nach der Verarbeitung der E-Mail aber feststellt, dass die E-Mail nicht zustellbar ist (und eine Unzustellbarkeitsbenachrichtigung auslöst). Da es sich jedoch um verschiedene Benachrichtigungstypen handelt, werden immer separate Benachrichtigungen gesendet.
- SES behält sich das Recht vor, den Benachrichtigungen zusätzliche Felder hinzuzufügen. Deshalb müssen Anwendungen, die diese Benachrichtigungen analysieren, in der Lage sein, unbekannte Felder zu verarbeiten.
- SES überschreibt die Kopfzeilen der Nachricht, wenn es die E-Mail sendet. Sie können die Header der ursprünglichen Nachricht aus den Feldern `headers` und `commonHeaders` des `mail`-Objekts abrufen.

JSON-Objekt der obersten Ebene

Das JSON-Objekt der obersten Ebene in einer SES-Benachrichtigung enthält die folgenden Felder.

Feldname	Description
`notificationType`	Eine Zeichenfolge, die den Typ der Benachric htigung enthält, der vom JSON-Objekt dargestellt wird. Die möglichen Werte sind `Bounce`, `Complaint` oder `Delivery`. Wenn Sie Einrichten der Ereignisveröffentl ichung wählen, heißt dieses Feld `eventType` .
`mail`	Ein JSON-Objekt, das Informationen zur ursprünglichen E-Mail enthält, auf die sich die Benachrichtigung bezieht. Weitere Informati onen finden Sie unter Mail-Objekt.
`bounce`	Dieses Feld ist nur dann vorhanden, wenn `notificationType` `Bounce` ist, und enthält ein JSON-Objekt mit Informationen über die Unzustellbarkeit. Weitere Informationen finden Sie unter Bounce-Objekt.
`complaint`	Dieses Feld ist nur dann vorhanden, wenn `notificationType` `Complaint` ist, und enthält ein JSON-Objekt mit Informationen zur Beschwerde. Weitere Informationen finden Sie unter Complaint-Objekt.
`delivery`	Dieses Feld ist nur dann vorhanden, wenn `notificationType` `Delivery` ist, und enthält ein JSON-Objekt mit Informationen zur Zustellung. Weitere Informationen finden Sie unter Delivery-Objekt.

Mail-Objekt

Jede Benachrichtigung über eine Unzustellbarkeit, Beschwerde oder Lieferung enthält Informationen über die ursprüngliche E-Mail-Benachrichtigung im `mail`-Objekt. Das JSON-Objekt enthält Informationen über ein `mail`-Objekt mit den folgenden Feldern.

Feldname	Description
`timestamp`	Der Zeitpunkt, zu dem die ursprüngliche Nachricht gesendet wurde (im ISO8601 Format).
`messageId`	Eine eindeutige ID, die SES der Nachricht zugewiesen hat. SES hat Ihnen diesen Wert zurückgegeben, als Sie die Nachricht gesendet haben. **Note** Diese Nachrichten-ID wurde von SES zugewiesen. Sie finden diese Mitteilungs-ID in der ursprünglichen E-Mail in den Feldern `headers` des `mail`-Objekts.
`source`	Die E-Mail-Adresse, von der die ursprüngliche Nachricht gesendet wurde (die Envelope-MAIL-FROM-Adresse).
`sourceArn`	Der Amazon-Ressourcenname (ARN) der Identität, die zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt `sourceArn` den ARN der ID an, die – gemäß Autorisierung durch den Identitätsbesitzer – vom stellvertretenden Sender zum Senden der E-Mail verwendet werden soll. Weitere

Feldname	Description
	Informationen zur Sendeautorisierung finden Sie unter E-Mail-Authentifizierungsmethoden.
`sourceIp`	Die ursprüngliche öffentliche IP-Adresse des Clients, der die E-Mail-Versandanfrage an SES ausgeführt hat.
`sendingAccountId`	Die AWS-Konto ID des Kontos, das zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt `sendingAccountId` die Konto-ID des stellvertretenden Senders an.
`callerIdentity`	Die IAM-Identität des SES-Benutzers, der die E-Mail gesendet hat.
`destination`	Eine Liste der E-Mail-Adressen, an die die ursprüngliche E-Mail gesendet wurde.
`headersTruncated`	Dieses Objekt ist nur vorhanden, wenn Sie die Benachrichtigungseinstellungen so konfiguriert haben, dass die Header der ursprünglichen E-Mail eingeschlossen werden. Gibt an, ob die Kopfzeilen in der Benachrichtigung abgeschnitten werden. SES kürzt die Kopfzeilen in der Benachrichtigung, wenn die Kopfzeilen der ursprünglichen Nachricht mindestens 10 KB groß sind. Mögliche Werte sind `true` und `false`.

Feldname	Description
`headers`	Dieses Objekt ist nur vorhanden, wenn Sie die Benachrichtigungseinstellungen so konfiguriert haben, dass die Header der ursprünglichen E-Mail eingeschlossen werden. Eine Liste der ursprünglichen Header der E-Mail. Jeder Header in der Liste verfügt über die Felder `name` und `value`. **Note** Jede Nachrichten-ID innerhalb des `headers` Objekts stammt aus der ursprünglichen Nachricht, die Sie an SES übergeben haben. Die Nachricht en-ID, die SES der Nachricht anschließ end zugewiesen hat, befindet sich im `messageId` Feld des `mail` Objekts.

Feldname	Description
`commonHeaders`	Dieses Objekt ist nur vorhanden, wenn Sie die Benachrichtigungseinstellungen so konfiguriert haben, dass die Header der ursprünglichen E-Mail eingeschlossen werden. Enthält Informationen über häufig verwendete E-Mail-Header aus der ursprünglichen E-Mail, einschließlich der Felder für den Absender, Empfänger und den Betreff. Innerhalb dieses Objekt ist jeder Header ein Schlüssel. Die Absender- und Empfängerfelder werden durch Arrays repräsentiert, die mehrere Werte enthalten. **Note** Bei Ergeinissen ist dies die Nachrichten-ID im Feld `commonHeaders` ist die Nachrichten-ID, die Amazon SES der Nachricht später im Feld `messageId` des Mail-Objekts zugewiesen hat. Benachrichtigungen enthalten die Nachrichten-ID der ursprünglichen E-Mail.

Im Folgenden finden Sie ein Beispiel eines `mail`-Objekts, das die Header der ursprünglichen E-Mail enthält. Wenn dieser Benachrichtigungstyp nicht so konfiguriert wurde, dass die ursprünglichen E-Mail-Header eingeschlossen werden, enthält das `mail`-Objekt die Felder `headersTruncated`, `headers` und `commonHeaders` nicht.

```
{
   "timestamp":"2018-10-08T14:05:45 +0000",
   "messageId":"000001378603177f-7a5433e7-8edb-42ae-af10-f0181f34d6ee-000000",
   "source":"sender@example.com",
   "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
```

```
    "sourceIp": "127.0.3.0",
    "sendingAccountId":"123456789012",
    "destination":[
       "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
       {
          "name":"From",
          "value":"\"Sender Name\" <sender@example.com>"
       },
       {
          "name":"To",
          "value":"\"Recipient Name\" <recipient@example.com>"
       },
       {
          "name":"Message-ID",
          "value":"custom-message-ID"
       },
       {
          "name":"Subject",
          "value":"Hello"
       },
       {
          "name":"Content-Type",
          "value":"text/plain; charset=\"UTF-8\""
       },
       {
          "name":"Content-Transfer-Encoding",
          "value":"base64"
       },
       {
          "name":"Date",
          "value":"Mon, 08 Oct 2018 14:05:45 +0000"
       }
    ],
    "commonHeaders":{
       "from":[
          "Sender Name <sender@example.com>"
       ],
       "date":"Mon, 08 Oct 2018 14:05:45 +0000",
       "to":[
          "Recipient Name <recipient@example.com>"
       ],
```

```
      "messageId":" custom-message-ID",
      "subject":"Message sent using SES"
   }
}
```

Bounce-Objekt

Das JSON-Objekt, das Informationen zu Unzustellbarkeiten enthält, weist die folgenden Felder auf.

Feldname	Description
`bounceType`	Die Art des Bounces, wie von SES festgeleg t. Weitere Informationen finden Sie unter Unzustellbarkeitstypen.
`bounceSubType`	Der Subtyp des Bounces, wie von SES bestimmt. Weitere Informationen finden Sie unter Unzustellbarkeitstypen.
`bouncedRecipients`	Eine Liste mit Informationen über die Empfänger der ursprünglichen E-Mail, an die diese nicht zugestellt werden konnte. Weitere Informationen finden Sie unter Empfänger, an die nicht zugestellt werden konnte.
`timestamp`	Das Datum und die Uhrzeit, zu denen der Bounce gesendet wurde (im ISO8601 Format). Beachten Sie, dass dies die Uhrzeit ist, zu der die Benachrichtigung vom ISP gesendet wurde, und nicht die Uhrzeit, zu der sie bei SES eingegangen ist.
`feedbackId`	Eine eindeutige ID für die Unzustellbarkeit.

Wenn SES in der Lage war, die Remote Message Transfer Authority (MTA) zu kontaktieren, ist das folgende Feld ebenfalls vorhanden.

Feldname	Description
`remoteMtaIp`	Die IP-Adresse des MTA, an den SES versucht hat, die E-Mail zuzustellen.

Wurde der Unzustellbarkeitsbenachrichtigung eine Zustellungsstatusbenachrichtigung (DSN, Delivery Status Notification) angefügt, ist auch das folgende Feld enthalten.

Feldname	Description
`reportingMTA`	Der Wert des `Reporting-MTA` -Felds der DSN. Dies ist der Wert der MTA, die versucht hat, die Zustellungs-, Weiterleitungs- oder Gateway-Operation durchzuführen, die in der DSN beschrieben ist.

Es folgt ein Beispiel für ein `bounce`-Objekt.

```
{
   "bounceType":"Permanent",
   "bounceSubType": "General",
   "bouncedRecipients":[
      {
         "status":"5.0.0",
         "action":"failed",
         "diagnosticCode":"smtp; 550 user unknown",
         "emailAddress":"recipient1@example.com"
      },
      {
         "status":"4.0.0",
         "action":"delayed",
         "emailAddress":"recipient2@example.com"
      }
   ],
   "reportingMTA": "example.com",
   "timestamp":"2012-05-25T14:59:38.605Z",
   "feedbackId":"000001378603176d-5a4b5ad9-6f30-4198-a8c3-b1eb0c270a1d-000000",
   "remoteMtaIp":"127.0.2.0"
```

```
}
```

Empfänger, an die nicht zugestellt werden konnte

Eine Benachrichtigung über die Unzustellbarkeit kann für einen einzelnen Empfänger oder für mehrere Empfänger gelten. Das `bouncedRecipients`-Feld enthält eine Liste von Objekten – eines pro Empfänger, für den die Benachrichtigung über die Unzustellbarkeit gilt – und weist zusätzlich immer das folgende Feld auf.

Feldname	Description
`emailAddress`	Die E-Mail-Adresse des Empfängers. Ist eine DSN verfügbar, ist dies der Wert des `Final-Recipient` -Felds der DSN.

Wurde eine DSN an eine Unzustellbarkeitsbenachrichtigung angehängt, sind möglicherweise folgende Felder ebenfalls vorhanden.

Feldname	Description
`action`	Der Wert des `Action`-Felds der DSN. Es zeigt die Aktion an, die von der berichtenden MTA als Reaktion auf die gescheiterte Zustellung der Benachrichtigung an diesen Empfänger ausgeführt wurde.
`status`	Der Wert des `Status`-Felds der DSN. Dies ist der vom Transport unabhängige Statuscod e pro Empfänger, der den Zustellstatus der Nachricht anzeigt.
`diagnosticCode`	Der vom berichtenden MTA gemeldete Statuscode. Dies ist der Wert des `Diagnosti c-Code` -Felds der DSN. Dieses Feld ist möglicherweise nicht im DSN und daher auch nicht in JSON enthalten.

Das folgende Beispiel zeigt ein Objekt, das möglicherweise in der `bouncedRecipients`-Liste enthalten ist.

```
{
    "emailAddress": "recipient@example.com",
    "action": "failed",
    "status": "5.0.0",
    "diagnosticCode": "X-Postfix; unknown user"
}
```

Unzustellbarkeitstypen

Das Bounce-Objekt enthält den Bounce-Typ`Undetermined`, `Permanent` (hart) oder `Transient` (weich). Die Bounce-Typen `Permanent` (Hard) und `Transient` (Soft) können auch einen von mehreren Bounce-Untertypen enthalten.

Wenn Sie eine Bounce-Benachrichtigung mit dem Bounce-Typ `Transient` (Soft) erhalten, können Sie möglicherweise in future eine E-Mail an diesen Empfänger senden, wenn das Problem, das zum Bounce der Nachricht geführt hat, behoben ist.

Wenn Sie eine Bounce-Benachrichtigung mit dem Bounce-Typ `Permanent` (schwer) erhalten, ist es unwahrscheinlich, dass Sie in future E-Mails an diesen Empfänger senden können. Aus diesem Grund sollten Sie sofort den Empfänger, dessen Adresse die Unzustellbarkeit erzeugt hat, aus Ihren Mailinglisten entfernen.

> **Note**
>
> Wenn ein Soft Bounce auftritt (ein Bounce, der auf ein vorübergehendes Problem zurückzuführen ist, z. B. wenn der Posteingang des Empfängers voll ist), versucht SES, die E-Mail für einen bestimmten Zeitraum erneut zuzustellen. Wenn SES die E-Mail am Ende dieses Zeitraums immer noch nicht zustellen kann, wird der Versuch eingestellt.
> SES sendet Benachrichtigungen für Hard Bounces und für Soft Bounces, die nicht mehr zugestellt wurden. Wenn Sie jedes Mal eine Benachrichtigung erhalten möchten, wenn eine temporäre Unzustellbarkeit auftritt, aktivieren Sie die Ereignisveröffentlichung und konfigurieren Sie sie so, dass Benachrichtigungen gesendet werden, wenn Zustellungsverzögerungsereignisse auftreten.

bounceType	bounceSubType	Description
`Undetermined`	`Undetermined`	Der E-Mail-Anbieter des Empfängers hat eine Unzustellbarkeitsnachricht gesendet. Die Bounce-Nachricht enthielt nicht genügend Informationen, damit SES den Grund für den Bounce ermitteln konnte. Die Unzustellbarkeits-E-Mail, die an die Adresse im Return-Path-Header der E-Mail gesendet wurde, die zur Unzustellbarkeit geführt hat, enthält möglicher weise zusätzliche Informationen zum Problem, das die Unzustellbarkeit der E-Mail verursacht hat.
`Permanent`	`General`	Der E-Mail-Anbieter des Empfängers hat eine Nachricht mit permanenter Unzustellbarkeit gesendet. **Important** Wenn Sie diese Art von Unzustell barkeitsbenachrichtigung erhalten, sollten Sie die E-Mail-Adresse des Empfängers sofort aus Ihrer Mailingliste entfernen. Das Senden von Nachricht en an Adressen, die permanente Unzustellbarkeiten erzeugen, kann negative Auswirkungen auf Ihren guten Ruf als Absender haben. Wenn Sie weiter E-Mails an Adressen senden, die permanente Unzustellbarkeiten erzeugen, können wir Ihre Fähigkeit, weitere E-Mails zu senden, vorüberge hend unterbrechen. Siehe the section called “Verwenden der Unterdrüc kungsliste auf Kontoebene”.

bounceType	bounceSubType	Description
`Permanent`	`NoEmail`	Es war nicht möglich, die E-Mail-Adresse des Empfängers aus der unzustellbaren Nachricht abzurufen.
`Permanent`	`Suppressed`	Die E-Mail-Adresse des Empfängers steht auf der SES-Unterdrückungsliste, da sie in jüngster Zeit zu Hard Bounces geführt hat. Informationen zum Überschreiben der globalen Unterdrückungsliste finden Sie unterVerwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole.
`Permanent`	`OnAccountSuppressionList`	SES hat das Senden an diese Adresse unterdrückt, da sie auf der Sperrliste auf Kontoebene steht. Dies zählt nicht für Ihre Unzustellbarkeitsraten-Metrik.

bounceType	bounceSubType	Description
`Permanent`	`UnsubscribedRecipient`	Dieser Bounce-Typ tritt auf, wenn der Kontakt des Empfängers das Thema abbestellt hat und ihm mithilfe der Listenverwaltungsoptionen eine E-Mail zugesandt wird. SES respektiert die Kontaktpräferenz und versucht nicht, sie zuzustellen. Außerdem wirkt sich diese Zurückweisung nicht auf die Reputation des Absenders aus, da die Zustellung nicht versucht wurde und der Kontakt des Empfängers aufgrund der Zurückweisung auch nicht zu einer Unterdrückungsliste hinzugefügt wurde. **Tip** Es wird empfohlen, UnsubscribedRecipient Ereignisse zu abonnieren, um zu vermeiden, dass weiterhin Nachrichten an Empfänger gesendet werden, die sich nicht angemeldet haben. Überlegen Sie. the section called “Verwenden von Listenverwaltung” Die Listenverwaltung sollte die Quelle der Wahrheit für Ihre Abonnentenliste sein. Aus Sicht der SES-Durchsetzung haben Sie den Ruf, sich nicht an bewährte Methoden für den E-Mail-Versand zu halten, wenn Sie weiterhin Nachrichten an unterdrückte oder abgemeldete Empfänger versenden.

bounceType	bounceSubType	Description
`Transient`	`General`	Der E-Mail-Anbieter des Empfängers hat eine allgemeine Unzustellbarkeitsnachricht gesendet. Sie können in Zukunft Nachrichten an denselben Empfänger senden, wenn das Problem, das zur Unzustellbarkeit führte, gelöst ist. **Note** Wenn Sie eine E-Mail an einen Empfänger senden, der über eine aktive automatische Antwortre gel (z. B. eine "außer Haus"-Abw esenheitsnachricht) verfügt, erhalten Sie möglicherweise diese Art von Benachrichtigung. Auch wenn die Antwort den Benachrichtigungst yp hat`Bounce`, zählt SES bei der Berechnung der Absprungrate für Ihr Konto keine automatischen Antworten.
`Transient`	`MailboxFull`	Der E-Mail-Anbieter des Empfängers hat eine Unzustellbarkeitsnachricht gesendet, da der Posteingang des Empfängers voll ist. Sie können in Zukunft Nachrichten an denselben Empfänger senden, sobald das Postfach nicht mehr voll ist.
`Transient`	`MessageTooLarge`	Der E-Mail-Anbieter des Empfängers hat eine Unzustellbarkeitsnachricht gesendet, da die Nachricht, die Sie gesendet haben, zu groß ist. Sie können Nachrichten an denselben Empfänger senden, wenn Sie die Größe der Nachricht reduzieren.

bounceType	bounceSubType	Description
`Transient`	`ContentRejected`	Der E-Mail-Anbieter des Empfängers hat eine Unzustellbarkeitsnachricht gesendet, da die von Ihnen gesendete Nachricht Inhalte enthält, die der Anbieter nicht erlaubt. Sie können Nachrichten an denselben Empfänger senden, wenn Sie den Inhalt der Nachricht ändern.
`Transient`	`AttachmentRejected`	Der E-Mail-Anbieter des Empfängers hat eine Unzustellbarkeitsnachricht gesendet, da die Nachricht einen nicht akzeptablen Anhang enthält. Beispiel: Einige E-Mail-Anbieter können Nachrichten mit Anhängen eines bestimmte n Dateityps oder Nachrichten mit sehr großen Anhängen ablehnen. Sie können Nachrichten an denselben Empfänger senden, wenn Sie den Inhalt des Anhangs entfernen oder ändern.

Complaint-Objekt

Das JSON-Objekt, das Informationen zu Beschwerden enthält, weist die folgenden Felder auf.

Feldname	Description
`complainedRecipients`	Eine Liste mit Informationen zu Empfänger n, die möglicherweise für die Beschwerde verantwortlich sind. Weitere Informationen finden Sie unter Empfänger, die sich beschwert haben.
`timestamp`	Das Datum und der Zeitpunkt, zu dem der ISP die Beschwerdebenachrichtigung gesendet hat, im Format ISO 8601. Das Datum und die Uhrzeit in diesem Feld stimmen möglicherweise nicht mit dem Datum und der Uhrzeit überein, an dem SES die Benachrichtigung erhalten hat.

Feldname	Description
`feedbackId`	Eine eindeutige ID, die mit der Beschwerde verknüpft ist.
`complaintSubType`	Der Wert des Feldes `complaintSubType` kann entweder null oder `OnAccount SuppressionList` sein. Wenn der Wert lautet`OnAccountSuppressionList`, hat SES die Nachricht akzeptiert, aber nicht versucht, sie zu senden, da sie auf der Sperrliste auf Kontoebene stand.

Ist zudem ein Feedback-Bericht an die Beschwerde angehängt, sind möglicherweise die folgenden Felder vorhanden.

Feldname	Description
`userAgent`	Der Wert des `User-Agent` -Felds aus dem Feedback-Bericht. Gibt den Namen und die Version des Systems an, das den Bericht generiert hat.
`complaintFeedbackType`	Der Wert des `Feedback-Type` -Felds aus dem Feedback-Bericht, der vom ISP empfangen wurde. Enthält die Art des Feedbacks.
`arrivalDate`	Der Wert des `Received-Date` Felds `Arrival-Date` oder aus dem Feedback-Bericht (im ISO8601 Format). Dieses Feld ist möglicherweise nicht im Bericht und daher auch nicht in JSON enthalten.

Es folgt ein Beispiel für ein `complaint`-Objekt.

```
{
   "userAgent":"ExampleCorp Feedback Loop (V0.01)",
   "complainedRecipients":[
      {
         "emailAddress":"recipient1@example.com"
      }
   ],
   "complaintFeedbackType":"abuse",
   "arrivalDate":"2009-12-03T04:24:21.000-05:00",
   "timestamp":"2012-05-25T14:59:38.623Z",
   "feedbackId":"000001378603177f-18c07c78-fa81-4a58-9dd1-fedc3cb8f49a-000000"
}
```

Empfänger, die sich beschwert haben

Das `complainedRecipients`-Feld enthält eine Liste von Empfängern, die sich möglicherweise beschwert haben. Anhand dieser Informationen sollten Sie ermitteln, welcher Empfänger die Beschwerde eingereicht hat, und diesen Empfänger dann sofort aus Ihren Mailinglisten entfernen.

> **Important**
>
> Die meisten ISPs entfernen die E-Mail-Adresse des Empfängers, der die Beschwerde eingereicht hat, aus ihrer Beschwerdebenachrichtigung. Aus diesem Grund enthält diese Liste Informationen zu Empfängern, die sich beschwert haben könnten. Dabei basiert die Einschätzung auf den Empfängern der ursprünglichen E-Mail und dem ISP, von dem wir die Beschwerde erhalten haben. SES führt eine Suche anhand der ursprünglichen Nachricht durch, um diese Empfängerliste zu ermitteln.

JSON-Objekte in dieser Liste enthalten das folgende Feld.

Feldname	Description
`emailAddress`	Die E-Mail-Adresse des Empfängers.

Es folgt ein Beispiel für ein Complained-Recipient-Objekt.

```
{ "emailAddress": "recipient1@example.com" }
```

> **Note**
>
> Aufgrund dieses Verhaltens können Sie besser einschätzen, von welchen E-Mail-Adressen Beschwerden über Ihre Nachricht kamen, wenn Sie das Senden auf eine Nachricht pro Empfänger beschränken (und nicht eine Nachricht an 30 verschiedene E-Mail-Adressen im Feld "BCC" senden).

Beschwerdetypen

Sie sehen möglicherweise die folgenden Beschwerdetypen im `complaintFeedbackType`-Feld, so wie sie vom meldenden ISP entsprechend der Website zu Internet Assigned Numbers Authority zugewiesen wurden:

- `abuse` – Weist auf eine unerwünschte E-Mail oder eine andere Art von E-Mail-Missbrauch hin.
- `auth-failure` – Bericht über einen E-Mail-Authentifizierungsfehler.
- `fraud` – Weist auf einen Betrug oder Phishing hin.
- `not-spam` – Weist darauf hin, dass die Entität, die den Bericht bereitstellt, die Nachricht nicht als Spam betrachtet. Dies kann verwendet werden, um eine Nachricht zu korrigieren, die fälschlicherweise als Spam gekennzeichnet oder kategorisiert wurde.
- `other` – Gibt eine andere Art von Feedback an, dass nicht zu den registrierten Typen passt.
- `virus` – Meldet, dass in der ursprünglichen Nachricht ein Virus entdeckt wurde.

Delivery-Objekt

Das JSON-Objekt, das die Informationen zu Zustellungen enthält, weist immer die folgenden Felder auf.

Feldname	Description
`timestamp`	Der Zeitpunkt, zu dem SES die E-Mail an den E-Mail-Server des Empfängers zugestellt hat (im ISO8601 Format).
`processingTimeMillis`	Die Zeit in Millisekunden zwischen der Annahme der Anfrage des Absenders durch

Feldname	Description
	SES und der Weiterleitung der Nachricht an den E-Mail-Server des Empfängers.
`recipients`	Eine Liste der beabsichtigten Empfänger der E-Mail, für die die Zustellungsbenachrichtigung gilt.
`smtpResponse`	Die SMTP-Antwortnachricht des Remote-ISP, der die E-Mail von SES akzeptiert hat. Diese Nachricht variiert je nach E-Mail, empfangen dem Mail-Server und empfangendem ISP.
`reportingMTA`	Der Hostname des SES-Mailservers, der die E-Mail gesendet hat.
`remoteMtaIp`	Die IP-Adresse des MTA, an den SES die E-Mail zugestellt hat.

Es folgt ein Beispiel für ein `delivery`-Objekt.

```
{
   "timestamp":"2014-05-28T22:41:01.184Z",
   "processingTimeMillis":546,
   "recipients":["success@simulator.amazonses.com"],
   "smtpResponse":"250 ok:  Message 64111812 accepted",
   "reportingMTA":"a8-70.smtp-out.amazonses.com",
   "remoteMtaIp":"127.0.2.0"
}
```

Amazon-SNS-Benachrichtigungsbeispiele für Amazon SES

Die folgenden Abschnitte enthalten Beispiele für die drei Arten von Benachrichtigungen:

- Beispiele für Unzustellbarkeitsbenachrichtigungen finden Sie unter Beispiele für Amazon-SNS-Unzustellbarkeitsbenachrichtigungen.
- Beispiele für Beschwerdebenachrichtigungen finden Sie unter Beispiele für Amazon-SNS-Beschwerdebenachrichtigungen.

- Beispiele für Zustellungsbenachrichtigungen finden Sie unter Beispiel einer Amazon-SNS-Zustellungsbenachrichtigung.

Beispiele für Amazon-SNS-Unzustellbarkeitsbenachrichtigungen

Dieser Abschnitt enthält Beispiele für Unzustellbarkeitsbenachrichtigungen mit und ohne Zustellungsstatusbenachrichtigung, bereitgestellt von dem E-Mail-Empfänger, der das Feedback gesendet hat.

Unzustellbarkeitsbenachrichtigung mit Zustellungsstatusbenachrichtigung

Es folgt ein Beispiel für eine Unzustellbarkeitsbenachrichtigung, die eine Zustellungsstatusbenachrichtigung und die ursprünglichen E-Mail-Header enthält. Wenn Unzustellbarkeitsbenachrichtigungen nicht so konfiguriert sind, dass sie die ursprünglichen E-Mail-Header enthalten, enthält das `mail`-Objekt innerhalb der Benachrichtigungen die Felder `headersTruncated`, `headers` und `commonHeaders` nicht.

```
{
    "notificationType":"Bounce",
    "bounce":{
       "bounceType":"Permanent",
       "reportingMTA":"dns; email.example.com",
       "bouncedRecipients":[
          {
             "emailAddress":"jane@example.com",
             "status":"5.1.1",
             "action":"failed",
             "diagnosticCode":"smtp; 550 5.1.1 <jane@example.com>... User"
          }
       ],
       "bounceSubType":"General",
       "timestamp":"2016-01-27T14:59:38.237Z",
       "feedbackId":"00000138111222aa-33322211-cccc-cccc-cccc-ddddaaaa068a-000000",
       "remoteMtaIp":"127.0.2.0"
    },
    "mail":{
       "timestamp":"2016-01-27T14:59:38.237Z",
       "source":"john@example.com",
       "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
       "sourceIp": "127.0.3.0",
       "sendingAccountId":"123456789012",
       "callerIdentity": "IAM_user_or_role_name",
```

```
          "messageId":"00000138111222aa-33322211-cccc-cccc-cccc-ddddaaaa0680-000000",
          "destination":[
            "jane@example.com",
            "mary@example.com",
            "richard@example.com"],
          "headersTruncated":false,
          "headers":[
           {
             "name":"From",
             "value":"\"John Doe\" <john@example.com>"
           },
           {
             "name":"To",
             "value":"\"Jane Doe\" <jane@example.com>, \"Mary Doe\" <mary@example.com>,
 \"Richard Doe\" <richard@example.com>"
           },
           {
             "name":"Message-ID",
             "value":"custom-message-ID"
           },
           {
             "name":"Subject",
             "value":"Hello"
           },
           {
             "name":"Content-Type",
             "value":"text/plain; charset=\"UTF-8\""
           },
           {
             "name":"Content-Transfer-Encoding",
             "value":"base64"
           },
           {
             "name":"Date",
             "value":"Wed, 27 Jan 2016 14:05:45 +0000"
           }
          ],
          "commonHeaders":{
             "from":[
                "John Doe <john@example.com>"
             ],
             "date":"Wed, 27 Jan 2016 14:05:45 +0000",
             "to":[
```

```
                "Jane Doe <jane@example.com>, Mary Doe <mary@example.com>, Richard Doe
<richard@example.com>"
            ],
            "messageId":"custom-message-ID",
            "subject":"Hello"
          }
       }
   }
```

Unzustellbarkeitsbenachrichtigung ohne Zustellungsstatusbenachrichtigung

Es folgt ein Beispiel für eine Unzustellbarkeitsbenachrichtigung, die die ursprünglichen E-Mail-Header, aber keine Zustellungsstatusbenachrichtigung enthält. Wenn Unzustellbarkeitsbenachrichtigungen nicht so konfiguriert sind, dass sie die ursprünglichen E-Mail-Header enthalten, enthält das `mail`-Objekt innerhalb der Benachrichtigungen die Felder `headersTruncated`, `headers` und `commonHeaders` nicht.

```
  {
     "notificationType":"Bounce",
     "bounce":{
        "bounceType":"Permanent",
        "bounceSubType": "General",
        "bouncedRecipients":[
           {
              "emailAddress":"jane@example.com"
           },
           {
              "emailAddress":"richard@example.com"
           }
        ],
        "timestamp":"2016-01-27T14:59:38.237Z",
        "feedbackId":"00000137860315fd-869464a4-8680-4114-98d3-716fe35851f9-000000",
        "remoteMtaIp":"127.0.2.0"
     },
     "mail":{
        "timestamp":"2016-01-27T14:59:38.237Z",
        "messageId":"00000137860315fd-34208509-5b74-41f3-95c5-22c1edc3c924-000000",
        "source":"john@example.com",
        "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
        "sourceIp": "127.0.3.0",
        "sendingAccountId":"123456789012",
        "callerIdentity": "IAM_user_or_role_name",
        "destination":[
```

```
            "jane@example.com",
            "mary@example.com",
            "richard@example.com"
         ],
        "headersTruncated":false,
        "headers":[
         {
            "name":"From",
            "value":"\"John Doe\" <john@example.com>"
         },
         {
            "name":"To",
            "value":"\"Jane Doe\" <jane@example.com>, \"Mary Doe\" <mary@example.com>,
\"Richard Doe\" <richard@example.com>"
         },
         {
            "name":"Message-ID",
            "value":"custom-message-ID"
         },
         {
            "name":"Subject",
            "value":"Hello"
         },
         {
            "name":"Content-Type",
            "value":"text/plain; charset=\"UTF-8\""
         },
         {
            "name":"Content-Transfer-Encoding",
            "value":"base64"
         },
         {
            "name":"Date",
            "value":"Wed, 27 Jan 2016 14:05:45 +0000"
          }
         ],
         "commonHeaders":{
           "from":[
              "John Doe <john@example.com>"
           ],
           "date":"Wed, 27 Jan 2016 14:05:45 +0000",
           "to":[
              "Jane Doe <jane@example.com>, Mary Doe <mary@example.com>, Richard Doe
<richard@example.com>"
```

```
          ],
          "messageId":"custom-message-ID",
          "subject":"Hello"
       }
    }
}
```

Beispiele für Amazon-SNS-Beschwerdebenachrichtigungen

Dieser Abschnitt enthält Beispiele für Beschwerdebenachrichtigungen mit und ohne Feedbackbericht, bereitgestellt von dem E-Mail-Empfänger, der das Feedback gesendet hat.

Beschwerdebenachrichtigung mit Feedbackbericht

Es folgt ein Beispiel für eine Beschwerdebenachrichtigungen, die einen Feedbackbericht und die ursprünglichen E-Mail-Header enthält. Wenn Beschwerdebenachrichtigungen nicht so konfiguriert sind, dass sie die ursprünglichen E-Mail-Header enthalten, enthält das `mail`-Objekt innerhalb der Benachrichtigungen die Felder `headersTruncated`, `headers` und `commonHeaders` nicht.

```
{
   "notificationType":"Complaint",
   "complaint":{
      "userAgent":"AnyCompany Feedback Loop (V0.01)",
      "complainedRecipients":[
         {
            "emailAddress":"richard@example.com"
         }
      ],
      "complaintFeedbackType":"abuse",
      "arrivalDate":"2016-01-27T14:59:38.237Z",
      "timestamp":"2016-01-27T14:59:38.237Z",
      "feedbackId":"000001378603177f-18c07c78-fa81-4a58-9dd1-fedc3cb8f49a-000000"
   },
   "mail":{
      "timestamp":"2016-01-27T14:59:38.237Z",
      "messageId":"000001378603177f-7a5433e7-8edb-42ae-af10-f0181f34d6ee-000000",
      "source":"john@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "sourceIp": "127.0.3.0",
      "sendingAccountId":"123456789012",
      "callerIdentity": "IAM_user_or_role_name",
      "destination":[
         "jane@example.com",
```

```
            "mary@example.com",
            "richard@example.com"
         ],
          "headersTruncated":false,
          "headers":[
           {
             "name":"From",
             "value":"\"John Doe\" <john@example.com>"
           },
           {
             "name":"To",
             "value":"\"Jane Doe\" <jane@example.com>, \"Mary Doe\" <mary@example.com>,
\"Richard Doe\" <richard@example.com>"
           },
           {
             "name":"Message-ID",
             "value":"custom-message-ID"
           },
           {
             "name":"Subject",
             "value":"Hello"
           },
           {
             "name":"Content-Type",
             "value":"text/plain; charset=\"UTF-8\""
           },
           {
             "name":"Content-Transfer-Encoding",
             "value":"base64"
           },
           {
             "name":"Date",
             "value":"Wed, 27 Jan 2016 14:05:45 +0000"
           }
         ],
         "commonHeaders":{
           "from":[
              "John Doe <john@example.com>"
           ],
           "date":"Wed, 27 Jan 2016 14:05:45 +0000",
           "to":[
              "Jane Doe <jane@example.com>, Mary Doe <mary@example.com>, Richard Doe
<richard@example.com>"
           ],
```

```
          "messageId":"custom-message-ID",
          "subject":"Hello"
       }
    }
}
```

Beschwerdebenachrichtigung ohne Feedbackbericht

Es folgt ein Beispiel für eine Beschwerdebenachrichtigung, die die ursprünglichen E-Mail-Header, aber keinen Feedbackbericht enthält. Wenn Beschwerdebenachrichtigungen nicht so konfiguriert sind, dass sie die ursprünglichen E-Mail-Header enthalten, enthält das `mail`-Objekt innerhalb der Benachrichtigungen die Felder `headersTruncated`, `headers` und `commonHeaders` nicht.

```
{
   "notificationType":"Complaint",
   "complaint":{
      "complainedRecipients":[
         {
            "emailAddress":"richard@example.com"
         }
      ],
      "timestamp":"2016-01-27T14:59:38.237Z",
      "feedbackId":"0000013786031775-fea503bc-7497-49e1-881b-a0379bb037d3-000000"
   },
   "mail":{
      "timestamp":"2016-01-27T14:59:38.237Z",
      "messageId":"0000013786031775-163e3910-53eb-4c8e-a04a-f29debf88a84-000000",
      "source":"john@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "sourceIp": "127.0.3.0",
      "sendingAccountId":"123456789012",
      "callerIdentity": "IAM_user_or_role_name",
      "destination":[
         "jane@example.com",
         "mary@example.com",
         "richard@example.com"
      ],
      "headersTruncated":false,
      "headers":[
       {
         "name":"From",
         "value":"\"John Doe\" <john@example.com>"
       },
```

```
          {
            "name":"To",
            "value":"\"Jane Doe\" <jane@example.com>, \"Mary Doe\" <mary@example.com>,
\"Richard Doe\" <richard@example.com>"
          },
          {
            "name":"Message-ID",
            "value":"custom-message-ID"
          },
          {
            "name":"Subject",
            "value":"Hello"
          },
          {
            "name":"Content-Type",
            "value":"text/plain; charset=\"UTF-8\""
          },
          {
            "name":"Content-Transfer-Encoding",
            "value":"base64"
          },
          {
            "name":"Date",
            "value":"Wed, 27 Jan 2016 14:05:45 +0000"
          }
          ],
          "commonHeaders":{
             "from":[
                "John Doe <john@example.com>"
             ],
             "date":"Wed, 27 Jan 2016 14:05:45 +0000",
             "to":[
                "Jane Doe <jane@example.com>, Mary Doe <mary@example.com>, Richard Doe
<richard@example.com>"
             ],
             "messageId":"custom-message-ID",
             "subject":"Hello"
          }
       }
    }
```

Beispiel einer Amazon-SNS-Zustellungsbenachrichtigung

Es folgt ein Beispiel für eine Zustellungsbenachrichtigung, die die ursprünglichen E-Mail-Header enthält. Wenn Zustellungsbenachrichtigungen nicht so konfiguriert sind, dass sie die ursprünglichen E-Mail-Header enthalten, enthält das `mail`-Objekt innerhalb der Benachrichtigungen die Felder `headersTruncated`, `headers` und `commonHeaders` nicht.

```
{
   "notificationType":"Delivery",
   "mail":{
      "timestamp":"2016-01-27T14:59:38.237Z",
      "messageId":"0000014644fe5ef6-9a483358-9170-4cb4-a269-f5dcdf415321-000000",
      "source":"john@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "sourceIp": "127.0.3.0",
      "sendingAccountId":"123456789012",
      "callerIdentity": "IAM_user_or_role_name",
      "destination":[
         "jane@example.com"
      ],
       "headersTruncated":false,
       "headers":[
        {
           "name":"From",
           "value":"\"John Doe\" <john@example.com>"
        },
        {
           "name":"To",
           "value":"\"Jane Doe\" <jane@example.com>"
        },
        {
           "name":"Message-ID",
           "value":"custom-message-ID"
        },
        {
           "name":"Subject",
           "value":"Hello"
        },
        {
           "name":"Content-Type",
           "value":"text/plain; charset=\"UTF-8\""
        },
        {
```

```
            "name":"Content-Transfer-Encoding",
            "value":"base64"
         },
         {
            "name":"Date",
            "value":"Wed, 27 Jan 2016 14:58:45 +0000"
         }
        ],
        "commonHeaders":{
          "from":[
             "John Doe <john@example.com>"
          ],
          "date":"Wed, 27 Jan 2016 14:58:45 +0000",
          "to":[
             "Jane Doe <jane@example.com>"
          ],
          "messageId":"custom-message-ID",
          "subject":"Hello"
        }
     },
    "delivery":{
       "timestamp":"2016-01-27T14:59:38.237Z",
       "recipients":["jane@example.com"],
       "processingTimeMillis":546,
       "reportingMTA":"a8-70.smtp-out.amazonses.com",
       "smtpResponse":"250 ok:  Message 64111812 accepted",
       "remoteMtaIp":"127.0.2.0"
    }
}
```

Verwenden der Identitätsautorisierung in Amazon SES

Identitätsautorisierungsrichtlinien definieren, wie einzelne verifizierte Identitäten Amazon SES verwenden können, indem sie angeben, welche SES-API-Aktionen unter welchen Bedingungen für die Identität zulässig sind oder verweigert werden.

Mit diesen Autorisierungsrichtlinien behalten Sie die Kontrolle über Ihre Identitäten, da Sie Berechtigungen jederzeit ändern oder widerrufen können. Sie können auch andere Benutzer autorisieren, Ihre Identitäten (Domains oder E-Mail-Adressen) mit ihren eigenen SES-Konten zu verwenden.

Themen

- Anatomie von Amazon-SES-Richtlinien
- Erstellen einer Identitätsautorisierungsrichtlinie in Amazon SES
- Beispiele für Identitätsrichtlinien in Amazon SES
- Verwalten Ihrer Identitätsautorisierungsrichtlinien in Amazon SES

Anatomie von Amazon-SES-Richtlinien

Richtlinien halten sich an eine bestimmte Struktur, enthalten Elemente und müssen bestimmte Anforderungen erfüllen.

Richtlinienstruktur

Bei jeder Autorisierungsrichtlinie handelt es sich um ein JSON-Dokument, das einer Identität angefügt wurde. Jede Richtlinie enthält folgende Abschnitte:

- Richtlinienweite Informationen oben im Dokument
- Eine oder mehrere einzelne Anweisungen, die jeweils eine Gruppe von Berechtigungen beschreiben

Die folgende Beispielrichtlinie gewährt der AWS Konto-ID 123456789012 die im Abschnitt Aktion angegebenen Berechtigungen für die verifizierte Domain example.com.

JSON

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeAccount",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
```

```
        "ses:GetEmailIdentity",
        "ses:UpdateEmailIdentityPolicy",
        "ses:ListRecommendations",
        "ses:CreateEmailIdentityPolicy",
        "ses:DeleteEmailIdentity"
      ]
    }
  ]
}
```

Weitere Beispiele für Autorisierungsrichtlinien finden Sie unter Beispiele für Identitätsrichtlinien.

Richtlinienelemente

Dieser Abschnitt beschreibt die Elemente von Identitätsautorisierungsrichtlinien. Zunächst beschreiben wir richtlinienweite Elemente und anschließend Elemente, die nur auf die Anweisung zutreffen, in der sie enthalten sind. Im Anschluss daran besprechen wir, wie Sie Ihren Anweisungen Bedingungen hinzufügen.

Ausführlichere Informationen über die Syntax der Elemente finden Sie unter Grammatik von IAM-Richtlinien im IAM Benutzerhandbuch.

Richtlinienweite Informationen

Es gibt zwei richtlinienweite Elemente: `Id` und `Version`. Die folgende Tabelle enthält Informationen über diese Elemente.

Name	Description	Erforderlich	Zulässige Werte
`Id`	Kennzeichnet die Richtlinie eindeutig.	Nein	Jede Zeichenfolge
`Version`	Gibt die Sprachversion des Richtlinienzugriffs an.	Nein	Jede Zeichenfolge. Als bewährte Methode empfehlen wir, dass Sie dieses Feld mit dem Wert "2012-10-17" einschließen.

Richtlinienspezifische Anweisungen

Identitätsautorisierungsrichtlinien erfordern mindestens eine Anweisung. Jede Anweisung kann die in der folgenden Tabelle beschriebenen Elementen enthalten.

Name	Description	Erforderlich	Zulässige Werte
`Sid`	Kennzeichnet die Anweisung eindeutig.	Nein	Jede Zeichenfolge.
`Effect`	Gibt das Ergebnis an, das die Richtlinienanweisung zum Bewertungszeitpunkt zurückgeben soll.	Ja	"Allow" oder "Deny".
`Resource`	Gibt die Identität an, auf die die Richtlinie zutrifft. (Für die Sendeautorisierung ist dies die E-Mail-Adresse oder Domain, für die der Identitätsbesitzer dem delegierten Sender die Berechtigung erteilt.)	Ja	Der Amazon-Ressourcenname (ARN) der Identität
`Principal`	Gibt den AWS-Konto Benutzer oder AWS Dienst an, der die in der Anweisung angegebene Berechtigung erhält.	Ja	Eine gültige AWS-Konto ID, Benutzer-ARN oder AWS Dienst. AWS-Konto IDs und Benutzer ARNs werden mit `"AWS"` (zum Beispiel `"AWS": ["123456789012"]`

Name	Description	Erforderlich	Zulässige Werte
			oder`"AWS": ["arn:aws:iam::123456789012:root"]`) angegeben. AWS Dienstnamen werden mit `"Service"` (zum Beispiel`"Service": ["cognito-idp.amazonaws.com"]`) angegeben. Beispiele für das ARNs Benutzerformat finden Sie unter Allgemeine AWS-Referenz.

Name	Description	Erforderlich	Zulässige Werte
`Action`	Gibt die Aktion an, für die die Anweisung gilt.	Ja	„ses: BatchGetMetricData „, „ses: „, CancelExportJob „ses: „, CreateDeliverabilityTestReport „ses: „, „ses: CreateEmailIdentityPolicy „, „ses: CreateExportJob „, „ses: „, DeleteEmailIdentity „ses: „, DeleteEmailIdentityPolicy „ses: „, "ses: GetDomainStatisticsReport „, „ses: GetEmailIdentity „, „ses: GetEmailIdentityPolicies „, „ses: „, GetExportJob „ses: „, „ses: ListExportJobs „, „ses: ListRecommendations „, „ses: PutEmailIdentityConfigurationSetAttributes „, „ses: „, PutEmailIdentityDkimAttributes „ses: „, „ses: PutEmailIdentityDkimSigningAttributes „, „ses: PutEmailIdentityFeedbackAttributes „, „ses: PutEmailIdentityMailFromAtt

Name	Description	Erforderlich	Zulässige Werte
			ributes „, „ses: „, TagResource „ses: „, „ses: UntagResource „, „ses:UpdateEmailIdentityPolicy“ (Autorisierungsaktionen senden: „ses: SendEmail „, „ses: SendRawEmail „, „ses: SendTemplatedEmail „, „ses: SendBulkTemplatedEmail „) Sie können eine oder mehrere dieser Operationen angeben.
`Condition`	Gibt alle Einschränkungen oder Details über die Berechtigung an.	Nein	Weitere Informationen über Bedingungen finden Sie im Anschluss an diese Tabelle.

Bedingungen

Bei einer Bedingung handelt es sich um jegliche Einschränkung, die die Berechtigung in der Anweisung betrifft. Der Teil der Anweisung, der die Bedingungen festlegt, kann der ausführlichste aller Bestandteile sein. Ein Schlüssel ist die Besonderheit, die die Grundlage für die Zugriffsbeschränkung, z. B. das Datum und die Uhrzeit der Anfrage, darstellt.

Sie verwenden Bedingungen und Schlüssel zusammen, um die Einschränkung auszudrücken. Wenn Sie beispielsweise den stellvertretenden Sender davon abhalten möchten, nach dem 30. Juli 2019 in Ihrem Namen Anfragen an Amazon SES zu stellen, verwenden Sie die Bedingung namens

`DateLessThan`. Sie verwenden den Schlüssel `aws:CurrentTime` und legen den Wert mit `2019-07-30T00:00:00Z` fest.

SES implementiert nur die folgenden Richtlinienschlüssel für AWS alle Bereiche:

- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:UserAgent`
- `aws:VpcSourceIp`

Weitere Informationen zu diesen Schlüsseln finden Sie im IAM-Benutzerhandbuch.

Politische Anforderungen

Richtlinien müssen alle folgenden Anforderungen erfüllen:

- Jede Richtlinie muss mindestens eine Anweisung enthalten.
- Jede Richtlinie muss mindestens über einen gültigen Prinzipal verfügen.
- Jede Richtlinie muss eine Ressource angeben und diese Ressource muss der ARN der Identität sein, der die Richtlinie zugeordnet ist.
- Identitätsbesitzer können jeder eindeutigen Identität bis zu 20 Richtlinien zuordnen.
- Richtlinien dürfen die Größe von 4 KB nicht überschreiten.
- Richtliniennamen dürfen 64 Zeichen nicht überschreiten. Darüber hinaus dürfen sie nur alphanumerische Zeichen, Bindestriche und Unterstriche enthalten.

Erstellen einer Identitätsautorisierungsrichtlinie in Amazon SES

Eine Identitätsautorisierungsrichtlinie besteht aus Anweisungen, die angeben, welche API-Aktionen unter welchen Bedingungen für eine Identität zulässig sind oder verweigert werden.

Um eine Amazon-SES-Domain- oder -E-Mail-Adressidentität in Ihrem Besitz zu autorisieren, erstellen Sie eine Autorisierungsrichtlinie und fügen diese Richtlinie dann der Identität an. Eine Identität kann

null, eine oder viele Richtlinien haben. Eine einzelne Richtlinie kann jedoch nur mit einer einzigen Identität verknüpft werden.

Eine Liste der API-Aktionen, die in einer Identitätsautorisierungsrichtlinie verwendet werden können, finden Sie in der Zeile Action in der Tabelle the section called “Richtlinienspezifische Anweisungen”.

Sie können eine Identitätsautorisierungsrichtlinie auf folgende Weisen erstellen:

- Mit dem Richtliniengenerator – Sie können eine einfache Richtlinie mithilfe des Richtliniengenerators in der SES-Konsole erstellen. Sie können nicht nur Berechtigungen für SES-API-Aktionen zulassen oder verweigern, sondern die Aktionen auch mit Bedingungen einschränken. Sie können den Richtliniengenerator auch zum schnellen Erstellen der grundlegenden Struktur einer Richtlinie verwenden und diese zu einem späteren Zeitpunkt anpassen, indem Sie die Richtlinie bearbeiten.
- Durch Erstellen einer benutzerdefinierten Richtlinie — Wenn Sie erweiterte Bedingungen einbeziehen oder einen AWS Dienst als Prinzipal verwenden möchten, können Sie eine benutzerdefinierte Richtlinie erstellen und sie mithilfe der SES-Konsole oder der SES-API an die Identität anhängen.

Themen

- Verwenden des Richtliniengenerators
- Erstellen einer benutzerdefinierten Richtlinie

Verwenden des Richtliniengenerators

Sie können den Richtliniengenerator verwenden, um eine einfache Autorisierungsrichtlinie zu erstellen, indem Sie diese Schritte ausführen.

So erstellen Sie eine Richtlinie mit dem Richtliniengenerator

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie im Container Identitäten auf dem Bildschirm Identitäten die verifizierte Identität aus, für die Sie eine Autorisierungsrichtlinie erstellen möchten.
4. Wählen Sie im Detailfenster der verifizierten Identität, die Sie im vorherigen Schritt ausgewählt haben, die Registerkarte Authorization (Autorisierung).

5. Wählen Sie im Bereich Authorization policies (Autorisierungsrichtlinien) Create policy (Richtlinie erstellen) und anschließend in der Drop-down-Liste Use policy generator (Richtliniengenerator verwenden) aus.
6. Wählen Sie im Bereich Create statement (Anweisung erstellen) im Feld Effect (Effekt) die Option Allow (Erlauben) aus. (Wenn Sie eine Richtlinie zum Einschränken dieser Identität erstellen möchten, wählen Sie stattdessen Deny (Verweigern) aus.)
7. Geben Sie im Feld Principals die AWS-Konto ID, den IAM-Benutzer-ARN oder den AWS Dienst ein, um die Berechtigungen zu erhalten, die Sie für diese Identität autorisieren möchten, und wählen Sie dann Hinzufügen aus. (Wenn Sie mehr als eine autorisieren möchten, wiederholen Sie diesen Schritt jeweils.)
8. Aktivieren Sie im Feld Actions (Aktionen) das Kontrollkästchen für jede Aktion, die Sie für Ihre Prinzipale autorisieren möchten.
9. (Optional) Erweitern Sie Specify conditions (Bedingungen angeben), wenn Sie der Berechtigung eine qualifizierende Anweisung hinzufügen möchten.

    a. Wählen Sie einen Operator aus der Dropdown-Liste Operator aus.
    b. Wählen Sie einen Typ aus der Dropdown-Liste Key (Schlüssel) aus.
    c. Geben Sie den Wert des ausgewählten Schlüsseltyps in das Feld Value (Wert) ein. (Wenn Sie weitere Bedingungen hinzufügen möchten, wählen Sie Add new condition (Neue Bedingung hinzufügen) und wiederholen Sie diesen Schritt für jede weitere.)
10. Wählen Sie Save statement (Anweisung speichern) aus.
11. (Optional) Erweitern Sie Create another statement (Eine weitere Anweisung erstellen), wenn Sie Ihrer Richtlinie weitere Anweisungen hinzufügen möchten und wiederholen Sie die Schritte 6 - 10.
12. Wählen Sie Next (Weiter) und auf dem Bildschirm Cutomize policy (Richtlinie anpassen) enthält der Container Edit policy details (Richtliniendetails bearbeiten) Felder, in denen Sie Name der Richtlinie und das Policy document (Richtliniendokument) selbst ändern oder anpassen können.
13. Wählen Sie Next (Weiter) aus. Auf dem Bildschirm Review and apply (Überprüfen und anwenden) zeigt der Container Overview (Übersicht) die verifizierte Identität, die Sie autorisieren, sowie den Namen dieser Richtlinie an. Im Bereich Policy document (Richtliniendokument) wird die aktuelle Richtlinie, die Sie gerade geschrieben haben, zusammen mit den von Ihnen hinzugefügten Bedingungen angezeigt. Überprüfen Sie die Richtlinie und wählen Sie Apply policy (Richtlinie anwenden), wenn sie richtig aussieht. (Wenn Sie etwas ändern oder korrigieren müssen, wählen Sie Previous (Zurück) und arbeiten Sie im Container Edit policy details (Richtliniendetails bearbeiten).)

Erstellen einer benutzerdefinierten Richtlinie

Wenn Sie eine benutzerdefinierte Richtlinie erstellen und Sie einer Identität anfügen möchten, haben Sie die folgenden Optionen:

- Mithilfe der Amazon-SES-API – Erstellen Sie eine Richtlinie in einem Texteditor, und fügen Sie die Richtlinie dann mithilfe der in der Amazon-Simple-Email-Service-API-Referenz beschriebenen `PutIdentityPolicy`API an die Identität an.
- Mithilfe der Amazon-SES-Konsole – Erstellen Sie die Richtlinie in einem Texteditor und fügen Sie sie anschließend einer Identität hinzu, indem Sie die Richtlinie in den Editor für benutzerdefinierte Richtlinien in der Amazon-SES-Konsole einfügen. Im folgenden Abschnitt wird diese Methode beschrieben.

So erstellen Sie eine benutzerdefinierte Richtlinie mit dem Editor für benutzerdefinierte Richtlinien

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie im Container Identitäten auf dem Bildschirm Identitäten die verifizierte Identität aus, für die Sie eine Autorisierungsrichtlinie erstellen möchten.
4. Wählen Sie im Detailfenster der verifizierten Identität, die Sie im vorherigen Schritt ausgewählt haben, die Registerkarte Authorization (Autorisierung).
5. Wählen Sie im Bereich Authorization policies (Autorisierungsrichtlinien) Create policy (Richtlinie erstellen) und anschließend in der Drop-down-Liste Create custom policy (Benutzerdefinierte Richtlinie erstellen) aus.
6. Geben oder fügen Sie im Bereich Policy document (Richtliniendokument) den Text Ihrer Richtlinie im JSON-Format ein. Sie können den Richtliniengenerator auch zum schnellen Erstellen der grundlegenden Struktur einer Richtlinie verwenden und diese anschließend hier anpassen.
7. Klicken Sie auf Apply Policy (Richtlinie anwenden). (Wenn Sie Ihre benutzerdefinierte Richtlinie jemals ändern müssen, aktivieren Sie einfach das Kontrollkästchen auf der Registerkarte Authorization (Autorisierung), wählen Sie Edit (Bearbeiten) und nehmen Sie Ihre Änderungen im Bereich Policy document (Richtliniendokument) vor und Save changes (Änderungen speichern) vor).

Beispiele für Identitätsrichtlinien in Amazon SES

Mit der Identitätsautorisierung können Sie die detaillierten Bedingungen angeben, unter denen Sie API-Aktionen für eine Identität zulassen oder verweigern.

Die folgenden Beispiele zeigen, wie Sie die Richtlinien erstellen müssen, um die verschiedenen Aspekte von API-Aktionen zu kontrollieren:

- Angeben des Prinzipals
- Einschränken der Aktion
- Verwenden mehrerer Anweisungen

Angeben des Prinzipals

Der Principal, also die Entität, der Sie die Berechtigung erteilen, kann ein AWS-Konto AWS Identity and Access Management (IAM-) Benutzer oder ein AWS Dienst sein, der zu demselben Konto gehört.

Das folgende Beispiel zeigt eine einfache Richtlinie, die es der AWS ID 123456789012 ermöglicht, die verifizierte Identität example.com zu kontrollieren, die ebenfalls 123456789012 gehört. AWS-Konto

JSON

```
{
  "Id":"SampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeMarketer",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:DeleteEmailIdentity",
        "ses:PutEmailIdentityDkimSigningAttributes"
```

```
      ]
    }
  ]
}
```

Die folgende Beispielrichtlinie erteilt zwei Benutzern die Berechtigung, die verifizierte Identität example.com zu kontrollieren. Die Benutzer werden durch ihren Amazon-Ressourcennamen (ARN) angegeben.

JSON

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeIAMUser",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::123456789012:user/John",
          "arn:aws:iam::123456789012:user/Jane"
        ]
      },
      "Action":[
        "ses:DeleteEmailIdentity",
        "ses:PutEmailIdentityDkimSigningAttributes"
      ]
    }
  ]
}
```

Einschränken der Aktion

Es gibt verschiedene Aktionen, die in einer Identitätsautorisierungsrichtlinie festgelegt werden können, je nachdem, welche Kontrollebene Sie autorisieren möchten:

```
"BatchGetMetricData",
"ListRecommendations",
```

```
"CreateDeliverabilityTestReport",
"CreateEmailIdentityPolicy",
"DeleteEmailIdentity",
"DeleteEmailIdentityPolicy",
"GetDomainStatisticsReport",
"GetEmailIdentity",
"GetEmailIdentityPolicies",
"PutEmailIdentityConfigurationSetAttributes",
"PutEmailIdentityDkimAttributes",
"PutEmailIdentityDkimSigningAttributes",
"PutEmailIdentityFeedbackAttributes",
"PutEmailIdentityMailFromAttributes",
"TagResource",
"UntagResource",
"UpdateEmailIdentityPolicy"
```

Mithilfe von Identitätsautorisierungsrichtlinien können Sie den Prinzipal auch auf nur eine dieser Aktionen einschränken.

JSON

```
{
    "Id": "ExamplePolicy",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ControlAction",
            "Effect": "Allow",
            "Resource": "arn:aws:ses:us-east-1:123456789012:identity/
example.com",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            },
            "Action": [
                "ses:PutEmailIdentityMailFromAttributes"
            ]
        }
    ]
}
```

Verwenden mehrerer Anweisungen

Ihre Identitätsautorisierungsrichtlinie kann mehrere Anweisungen enthalten. Die folgende Beispielrichtlinie enthält zwei Anweisungen. Die erste Aussage verweigert zwei Benutzern den Zugriff auf `getemailidentity` von sender@example.com innerhalb desselben Kontos `123456789012` aus. Die zweite Aussage verweigert `UpdateEmailIdentityPolicy` für den Prinzipal, Jack, innerhalb desselben Kontos `123456789012`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"DenyGet",
      "Effect":"Deny",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/
sender@example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::123456789012:user/John",
          "arn:aws:iam::123456789012:user/Jane"
        ]
      },
      "Action":[
        "ses:GetEmailIdentity"
      ]
    },
    {
      "Sid":"DenyUpdate",
      "Effect":"Deny",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/
sender@example.com",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:user/Jack"
      },
      "Action":[
        "ses:UpdateEmailIdentityPolicy"
      ]
    }
  ]
}
```

Verwalten Ihrer Identitätsautorisierungsrichtlinien in Amazon SES

Zusätzlich zum Erstellen und Anfügen von Richtlinien an Identitäten können Sie die Richtlinien einer Identität auch bearbeiten, entfernen, auflisten und abrufen, wie in den folgenden Abschnitten beschrieben.

Verwalten von Richtlinien mit der Amazon-SES-Konsole

Das Verwalten von Amazon-SES-Richtlinien beinhaltet das Anzeigen, Bearbeiten oder Löschen einer Richtlinie, die mit einer Identität verbunden ist, mit der Amazon-SES-Konsole.

So verwalten Sie Richtlinien mit der Amazon-SES-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, die Sie verwalten möchten.
4. Navigieren Sie auf der Detailseite der Identität zur Registerkarte Authorization (Autorisierung). Hier finden Sie eine Liste aller Richtlinien, die dieser Identität zugeordnet sind.
5. Wählen Sie die Richtlinie aus, die Sie verwalten möchten, indem Sie das Kontrollkästchen aktivieren.
6. Wählen Sie je nach gewünschter Verwaltungsaufgabe die entsprechende Schaltfläche wie folgt aus:

    a. Um die Richtlinie anzuzeigen, wählen Sie View policy (Richtlinie anzeigen). Wenn Sie eine Kopie davon benötigen, klicken Sie auf Copy (Kopieren), um sie in die Zwischenablage zu kopieren.

    b. Um die Richtlinie zu bearbeiten, wählen Sie Edit (Bearbeiten) aus. Bearbeiten Sie im Bereich Policy Dokument (Richtliniendokument) die Richtlinie, und wählen Sie dann Save changes (Änderungen speichern) aus.

    > **Note**
    >
    > Wenn Sie Berechtigungen widerrufen möchten, können Sie die Richtlinie entweder bearbeiten oder entfernen.

    c. Um die Richtlinie zu entfernen, wählen Sie Delete (Löschen) aus.

> **Important**
>
> Das Entfernen einer Richtlinie ist dauerhaft. Wir empfehlen, die Richtlinie vor dem Entfernen durch Kopieren und Einfügen in eine Textdatei zu sichern.

Verwalten von Richtlinien mit der Amazon-SES-API

Das Verwalten von Amazon-SES-Richtlinien beinhaltet das Anzeigen, Bearbeiten oder Löschen einer Richtlinie, die mit einer Identität verbunden ist, mit der Amazon-SES-API.

So listen Sie Richtlinien mithilfe der Amazon SES API auf und zeigen Sie sie an

- Mithilfe der ListIdentityPolicies API-Operation können Sie die Richtlinien auflisten, die mit einer Identität verknüpft sind. Sie können die Richtlinien auch selbst mithilfe der GetIdentityPoliciesAPI-Operation abrufen.

So bearbeiten Sie eine Richtlinie mit der Amazon-SES-API

- Sie können eine Richtlinie, die an eine Identität angehängt ist, mithilfe der PutIdentityPolicy API-Operation bearbeiten.

So löschen Sie eine Richtlinie mit der Amazon-SES-API

- Sie können eine Richtlinie, die mit einer Identität verknüpft ist, mithilfe der DeleteIdentityPolicy API-Operation löschen.

Verwenden der Sendeautorisierung mit Amazon SES

Sie können Amazon SES so konfigurieren, dass andere Benutzer autorisiert werden, E-Mails von Ihren eigenen Identitäten (Domänen oder E-Mail-Adressen) mit ihren eigenen Amazon-SES-Konten zu senden. Mit der Funktion Sendeautorisierung behalten Sie die Kontrolle über Ihre Identität, sodass Sie Berechtigungen jederzeit ändern oder widerrufen können. Als Besitzer eines Unternehmens können Sie beispielsweise mit der Sendeautorisierung einen Dritten (z. B. ein E-Mail-Marketing-Unternehmen) berechtigen, E-Mails von einer Domäne zu senden, die Sie besitzen.

In diesem Kapitel werden die Besonderheiten der Sendeautorisierung behandelt, die die veraltete Funktion für kontoübergreifende Benachrichtigungen ersetzt. Zunächst sollten Sie sich unter Verwenden der Identitätsautorisierung in Amazon SES mit den Grundlagen der identitätsbasierten Autorisierung mithilfe von Autorisierungsrichtlinien vertraut machen. In diesem Kapitel werden wichtige Themen wie die Anatomie einer Autorisierungsrichtlinie und die Verwaltung von Richtlinien behandelt.

Kontoübergreifender Legacy-Benachrichtigungssupport

Feedback-Benachrichtigungen für Unzustellbarkeiten, Beschwerden und Zustellungen im Zusammenhang mit E-Mails, die von einem delegierten Sender gesendet wurden, der von einem Identitätsbesitzer autorisiert wurde, von einer seiner verifizierten Identitäten zu senden, wurden traditionell mit kontoübergreifenden Benachrichtigungen konfiguriert, bei denen der delegierte Sender ein Thema einer Identität zuordnet, in deren Besitz er nicht ist (das bedeutet kontoübergreifend). Kontoübergreifende Benachrichtigungen wurden jedoch durch die Verwendung von Konfigurationssätzen und verifizierten Identitäten in Verbindung mit dem delegierten Senden ersetzt, wobei der delegierte Sender vom Identitätsbesitzer autorisiert wurde, eine seiner verifizierten Identitäten zum Senden von E-Mails zu verwenden. Diese neue Methode ermöglicht die Flexibilität, Unzustellbarkeits-, Beschwerde-, Zustellungs- und andere Ereignisbenachrichtigungen durch die folgenden zwei Konstrukte zu konfigurieren, je nachdem, ob Sie der delegierte Sender oder der Besitzer der verifizierten Identität sind:

- Konfigurationssätze – Der delegierte Sender kann die Veröffentlichung von Ereignissen in seinem eigenen Konfigurationssatz einrichten, den er angeben kann, wenn er E-Mails von einer verifizierten Identität sendet, die er nicht besitzt, aber vom Identitätsbesitzer über eine Autorisierungsrichtlinie gesendet werden darf. Durch die Veröffentlichung von Ereignissen können Benachrichtigungen über Bounce, Beschwerden, Lieferungen und andere Ereignisse auf Amazon CloudWatch, Amazon Data Firehose, Amazon Pinpoint und Amazon SNS veröffentlicht werden. Siehe Ereignisziele erstellen.
- Verifizierte Identitäten – Abgesehen davon, dass der Identitätsbesitzer den delegierten Sender autorisieren muss, eine seiner verifizierten Identitäten zum Senden von E-Mails zu verwenden, kann er auf Anfrage des delegierten Senders auch Feedbackbenachrichtigungen zur gemeinsamen Identität konfigurieren, um SNS-Themen zu verwenden, die dem delegierten Sender gehören. Nur der delegierte Sender erhält diese Benachrichtigungen, da er das SNS-Thema besitzt. In Schritt 14 erfahren Sie, wie Sie ein „SNS-Thema, das Ihnen nicht gehört“ in den Autorisierungsrichtlinienverfahren konfigurieren.

> **Note**
>
> Aus Gründen der Kompatibilität werden kontoübergreifende Benachrichtigungen für kontoübergreifende Legacy-Benachrichtigungen unterstützt, die derzeit in Ihrem Konto verwendet werden. Dieser Support beschränkt sich darauf, alle aktuellen kontoübergreifenden Konten zu ändern und zu verwenden, die Sie in der klassischen Amazon-SES-Konsole erstellt haben. Sie können jedoch keine neuen kontoübergreifenden Benachrichtigungen mehr erstellen. Um neue in der neuen Amazon-SES-Konsole zu erstellen, verwenden Sie die neuen Methoden zum delegierten Senden entweder mit Konfigurationssätzen, die Ereignisveröffentlichung verwenden, oder mit verifizierten Identitäten, die mit Ihren eigenen SNS-Themen konfiguriert sind.

Themen

- Übersicht über die Amazon-SES-Sendeautorisierung
- Aufgaben des Identitätsbesitzers für die Amazon-SES-Sendeautorisierung
- Delegieren der Senderaufgaben für die Amazon-SES-Sendeautorisierung

Übersicht über die Amazon-SES-Sendeautorisierung

Dieses Thema bietet eine Übersicht über den Vorgang der Sendeautorisierung und erklärt, wie die Amazon-SES-Funktionen zum Senden von E-Mails, z. B. Sendekontingente und Benachrichtigungen, in Bezug auf die Sendeautorisierung funktionieren.

In diesem Abschnitt werden die folgenden Begriffe verwendet:

- Identität – Eine E-Mail-Adresse oder Domäne, die Amazon-SES-Benutzer zur Versendung von E-Mails verwenden.
- Identitätsbesitzer – Ein Amazon-SES-Benutzer, der aufgrund der unter Verifizierte Identitäten beschriebenen Verfahren die verifizierte Eigentümerschaft über eine E-Mail-Adresse oder Domäne besitzt.
- Delegierter Absender — Ein AWS Konto, ein AWS Identity and Access Management (IAM-) Benutzer oder ein AWS Dienst, der durch eine Autorisierungsrichtlinie autorisiert wurde, E-Mails im Namen des Identitätsinhabers zu senden.

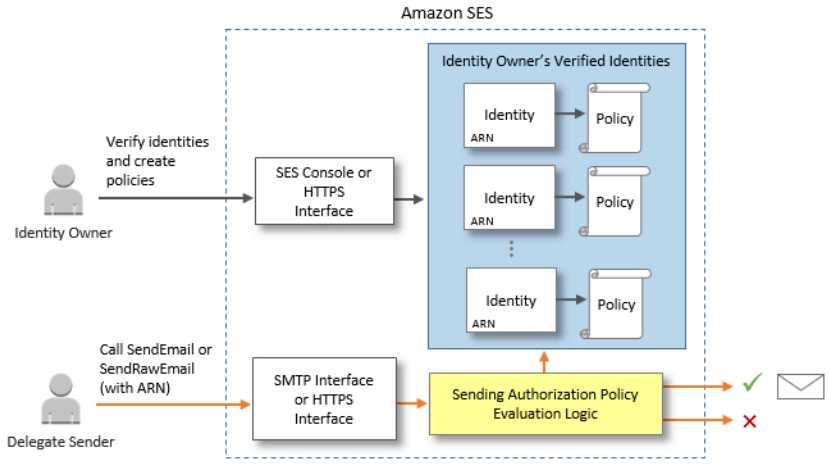
- Sendeautorisierungsrichtlinie – Ein Dokument, das Sie einer Identität anfügen können, um festzulegen, welche Benutzer für diese Identität und unter welchen Bedingungen E-Mails senden können
- Amazon Resource Name (ARN) — Eine standardisierte Methode zur eindeutigen Identifizierung einer AWS Ressource in allen AWS Services. Für die Sendeberechtigung ist die Ressource die Identität, deren Verwendung der Identitätsbesitzer dem delegierten Sender autorisiert hat. Hier sehen Sie ein Beispiel für einen ARN arn:aws:ses:us-east-1:123456789012:identity/example.com.

Sendeautorisierungsverfahren

Die Sendeautorisierung beruht auf den Sendeautorisierungsrichtlinien. Wenn Sie einem stellvertretenden Sender die Berechtigung erteilen möchten, E-Mails in Ihrem Auftrag senden zu können, müssen Sie eine Sendeautorisierungsrichtlinie erstellen, die Sie mithilfe der Amazon-SES-Konsole oder der Amazon-SES-API Ihrer Identität zuordnen. Wenn der stellvertretende Sender versucht, in Ihrem Namen eine E-Mail über Amazon SES zu senden, muss er den ARN Ihrer Identität in der Anfrage oder in der Kopfzeile der E-Mail übergeben.

Wenn Amazon SES die Anfrage zum Senden der E-Mail erhält, überprüft der Service die Richtlinie der Identität (sofern vorhanden), um festzustellen, ob Sie den stellvertretenden Sender autorisiert haben, im Namen der Identität E-Mails zu senden. Wenn der stellvertretende Sender autorisiert ist, akzeptiert Amazon SES die E-Mail, andernfalls gibt Amazon SES eine Fehlermeldung zurück.

Das folgende Diagramm zeigt die enge Beziehung zwischen den Konzepten der Sendeautorisierung:



Das Sendeautorisierungsverfahren besteht aus den folgenden Schritten:

1. Der Identitätsinhaber wählt eine verifizierte Identität aus, die der stellvertretende Sender verwenden soll. (Falls Sie keine Identität verifiziert haben, finden Sie Informationen unter Verifizierte Identitäten).

   > **Note**
   >
   > Der verifizierten Identität, die Sie für Ihren stellvertretenden Sender auswählen, darf kein Standardkonfigurationssatz zugewiesen sein.

2. Der Delegate-Absender teilt dem Identitätsinhaber mit, welche AWS Konto-ID oder welchen IAM-Benutzer-ARN er zum Senden verwenden möchte.
3. Wenn der Identitätsbesitzer zustimmt, dass der delegierte Sender von einem Konto des Besitzers aus senden darf, erstellt er eine Sendeautorisierungsrichtlinie und hängt die Richtlinie über die Amazon-SES-Konsole oder die Amazon-SES-API an die ausgewählte Identität an.
4. Der Identitätsbesitzer gibt dem delegierten Sender den ARN der autorisierten Identität, damit der delegierte Sender den ARN beim Senden der E-Mail an Amazon SES übermitteln kann.
5. Der delegierte Sender kann Unzustellbarkeits- und Beschwerdebenachrichtigungen über Event Publishing (Ereignisveröffentlichung) einrichten, die in einem Konfigurationssatz aktiviert ist, der beim delegierten Senden festgelegt wurde. Der Identitätsbesitzer kann auch E-Mail-Feedback-Benachrichtigungen für Unzustellbarkeits- und Beschwerdeereignisse einrichten, die an die Amazon-SNS-Themen des delegierten Senders gesendet werden.

   > **Note**
   >
   > Wenn der Identitätsinhaber das Senden von Ereignisbenachrichtigungen deaktiviert, muss der delegierte Absender die Ereignisveröffentlichung einrichten, um Bounce- und Beschwerdeereignisse in einem Amazon SNS SNS-Thema oder einem Firehose-Stream zu veröffentlichen. Der Sender muss ebenfalls den Konfigurationssatz, der die Ereignisveröffentlichungsregel enthält, auf jede E-Mail, die er sendet, anwenden. Wenn weder der Identitätsbesitzer noch der stellierte Absender eine Methode zum Senden von Benachrichtigungen für Unzustellbarkeits- und Beschwerdeereignisse einrichten, sendet Amazon SES automatisch Ereignisbenachrichtigungen per E-Mail an die Adresse im Feld „Antwortpfad bei Unzustellbarkeit“ der E-Mail (oder die Adresse im Feld „Quelle“, wenn Sie keine Absenderpfadadresse angegeben haben), selbst wenn der Identitätsbesitzer die Weiterleitung von E-Mail-Feedback deaktiviert hat.

6. Der stellvertretende Sender versucht, im Namen des Identitätsbesitzers eine E-Mail über Amazon SES zu senden, indem er den ARN der Identität des Identitätsbesitzers in der Anfrage oder in der Kopfzeile der E-Mail übergibt. Der stellvertretende Sender kann die E-Mail entweder über die Amazon-SES-SMTP-Schnittstelle oder die Amazon-SES-API senden. Nach Eingang der Anfrage untersucht Amazon SES alle Richtlinien, die der Identität angefügt wurden, und akzeptiert die E-Mail, wenn der stellvertretende Sender zur Verwendung der angegebenen „Von-“ und „Rücksendepfad-“ -Adresse autorisiert ist. Andernfalls gibt einen Fehler zurück und die Nachricht wird nicht akzeptiert.

   > **Important**
   >
   > Das AWS Konto des delegierten Absenders muss aus der Sandbox entfernt werden, bevor es zum Senden von E-Mails an nicht verifizierte Adressen verwendet werden kann.

7. Wenn der Identitätsbesitzer die Autorisierung des stellvertretenden Senders aufheben muss, muss der Identitätsbesitzer die Richtlinie für die Sendeautorisierung bearbeiten oder die Richtlinie vollständig löschen. Der Identitätsbesitzer kann jede dieser Aktionen über die Amazon-SES-Konsole oder die Amazon-SES-API ausführen.

Weitere Informationen darüber, wie der Identitätsbesitzer oder der delegierte Sender diese Aufgaben ausführt, finden Sie unter Aufgaben des Identitätsbesitzers bzw. Delegieren der Senderaufgaben.

Zuordnung der Funktionen für den E-Mail-Versand

Es ist wichtig, die Rolle des delegierten Senders und des Identitätsbesitzers in Bezug auf die Funktionen des Amazon-SES-E-Mail-Versands zu verstehen. Diese Funktionen umfassen beispielsweise die tägliche Sendequote, Unzustellbarkeitsnachrichten und Beschwerden, DKIM-Signatur, Feedback-Weiterleitung usw. Die Zuordnung erfolgt folgendermaßen:

- Sendequoten – E-Mails, die über die Identitäten des Identitätsbesitzers gesendet werden, werden auf die täglichen Sendekontingente des stellvertretenden Senders angerechnet.
- Unzustellbarkeitsnachrichten und Beschwerden – Unzustellbarkeits- und Beschwerdeereignisse werden für das Amazon-SES-Konto des stellvertretenden Senders dokumentiert und können sich daher auf die Reputation des stellvertretenden Senders auswirken.
- DKIM-Signatur – Wenn der Identitätsbesitzer die Easy DKIM-Signatur für eine Identität aktiviert hat, verfügen alle von dieser Identität gesendeten E-Mails über die DKIM-Signatur, einschließlich

E-Mails, die von dem stellvertretenden Sender gesendet wurden. Nur der Identitätsbesitzer kann steuern, ob die E-Mails mit einer DKIM-Signatur versehen werden.

- Benachrichtigungen – Sowohl der Identitätsbesitzer als auch der stellvertretende Sender kann Benachrichtigungen für Unzustellbarkeitsnachrichten und Beschwerden einrichten. Der E-Mail-Identitätsbesitzer kann auch die Weiterleitung von E-Mail-Feedback aktivieren. Weitere Informationen zum Einrichten von Benachrichtigungen finden Sie unter Überwachen Ihrer Amazon SES-Sendeaktivität.
- Verifizierung – Identitätsbesitzer müssen sicherstellen, dass sie die Verfahren unter Verifizierte Identitäten befolgen, um zu gewährleisten, dass sie die E-Mail-Adressen und Domänen auch tatsächlich besitzen, bevor sie delegierte Sender zu deren Verwendung autorisieren. Delegierte Sender müssen speziell für die Sendeautorisierung keine E-Mail-Adressen oder Domänen bestätigen.

  > **Important**
  >
  > Das AWS Konto des Absenders des Delegierten muss aus der Sandbox entfernt werden, bevor es zum Senden von E-Mails an nicht verifizierte Adressen verwendet werden kann.

- AWS Regionen — Der Absender des Delegierten muss die E-Mails aus der AWS Region senden, in der die Identität des Identitätsinhabers verifiziert wurde. Die Richtlinie für die Sendeautorisierung, die dem stellvertretenden Sender seine Berechtigung erteilt, muss der Identität in dieser Region angefügt sein.
- Fakturierung – Alle Nachrichten, die aus dem Konto des stellvertretenden Senders gesendet werden, einschließlich E-Mails, die der stellvertretende Sender unter Verwendung der Adressen des Identitätsbesitzers sendet, werden dem stellvertretenden Sender in Rechnung gestellt.

Aufgaben des Identitätsbesitzers für die Amazon-SES-Sendeautorisierung

Dieser Abschnitt beschreibt die Schritte, die Identitätsbesitzer bei der Konfiguration für die Autorisierung von Sendungen durchführen müssen.

Themen

- Bestätigen einer Identität für die Amazon-SES-Sendeautorisierung
- Einrichten der Benachrichtigungen für Identitätsbesitzer für die Amazon-SES-Sendeautorisierung
- Abrufen von Informationen vom delegierten Sender für die Amazon-SES-Sendeautorisierung
- Erstellen einer Sendeautorisierungsrichtlinie in Amazon SES

- Beispiele für Senderichtlinien
- Bereitstellen der Identitätsinformationen für den delegierten Sender im Zusammenhang mit der Amazon-SES-Sendeautorisierung

Bestätigen einer Identität für die Amazon-SES-Sendeautorisierung

Der erste Schritt bei der Konfiguration der Sendeautorisierung besteht darin, nachzuweisen, dass Sie die E-Mail-Adresse oder Domäne besitzen, die der stellvertretende Sender zum Senden der E-Mails verwendet. Das Verifizierungsverfahren wird unter Verifizierte Identitäten beschrieben.

Sie können überprüfen, ob eine E-Mail-Adresse oder Domain verifiziert ist, indem Sie ihren Status im Abschnitt Verifizierte Identitäten von https://console.aws.amazon.com/ses/oder mithilfe der `GetIdentityVerificationAttributes` API-Operation überprüfen.

Bevor Sie oder der stellvertretende Sender E-Mails an nicht verifizierte E-Mail-Adressen senden können, müssen Sie eine Anfrage senden, damit Ihr Konto aus der Amazon-SES-Sandbox entfernt wird. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).

> **Important**
>
> - Der Name AWS-Konto des delegierten Absenders muss aus der Sandbox entfernt werden, bevor er zum Senden von E-Mails an oder von nicht verifizierten Adressen verwendet werden kann.
> - Wenn sich Ihr Konto in der Sandbox befindet, können Sie keine E-Mails an E-Mail-Adressen senden, die in Ihrem Konto nicht verifiziert wurden, selbst wenn diese Domänen oder E-Mail-Adressen im Identitätskonto verifiziert wurden

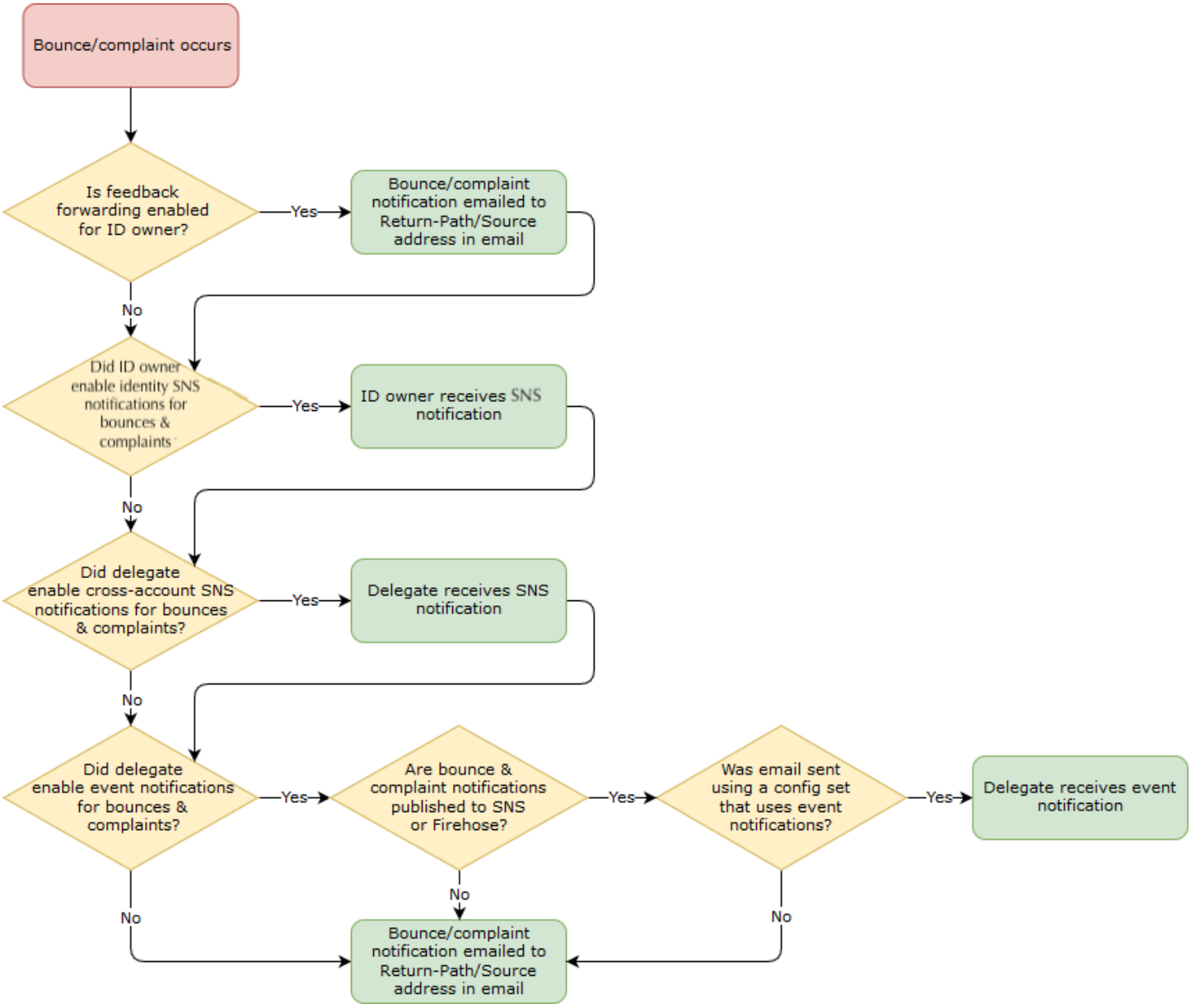
Einrichten der Benachrichtigungen für Identitätsbesitzer für die Amazon-SES-Sendeautorisierung

Wenn Sie einen stellvertretenden Sender autorisieren, in Ihrem Auftrag E-Mails zu versenden, rechnet Amazon SES alle Unzustellbarkeitsnachrichten und Beschwerden, die durch diese E-Mails generiert werden, den Unzustellbarkeits- und Beschwerdelimits des stellvertretenden Senders an und nicht den Ihren. Wenn Ihre IP-Adresse jedoch aufgrund von Nachrichten, die von einem delegierten Absender gesendet wurden, in DNS-basierten Anti-Spam-Listen (DNSBLs) von Drittanbietern erscheint, kann dies den Ruf Ihrer Identitäten schädigen. Aus diesem Grund sollten

Sie als Identitätsbesitzer eine E-Mail-Feedback-Weiterleitung für alle Ihre Identitäten einrichten, einschließlich derjenigen, die Sie zum delegierten Senden autorisiert haben. Weitere Informationen finden Sie unter Verwenden von Benachrichtigungen für den Amazon-SES-E-Mail-Empfang.

Delegierte Sender können ihre eigenen Unzustellbarkeits- und Beschwerdebenachrichtigungen für die Identitäten einrichten, für deren Verwendung sie von Ihnen autorisiert wurden. Sie können die Veröffentlichung von Ereignissen einrichten, um Bounce- und Beschwerdeereignisse in einem Amazon SNS SNS-Thema oder einem Firehose-Stream zu veröffentlichen.

Wenn weder der Identitätsbesitzer noch der stellierte Absender eine Methode zum Senden von Benachrichtigungen für Unzustellbarkeits- und Beschwerdeereignisse einrichten oder wenn der Absender den Konfigurationssatz, der die Ereignisveröffentlichungsregel verwendet, nicht anwendet, sendet Amazon SES automatisch Ereignisbenachrichtigungen per E-Mail an die Adresse im Feld „Antwortpfad bei Unzustellbarkeit“ der E-Mail (oder die Adresse im Feld Quelle, wenn Sie keine Return-Path-Adresse angegeben haben), auch wenn Sie die E-Mail-Feedback-Weiterleitung deaktiviert haben. Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Abrufen von Informationen vom delegierten Sender für die Amazon-SES-Sendeautorisierung

Ihre Sendeautorisierungsrichtlinie muss mindestens einen Prinzipal angeben, bei dem es sich um die Entität Ihres delegierten Senders handelt, dem Sie Zugriff gewähren, damit er im Namen einer Ihrer bestätigten Identitäten senden kann. Bei den Richtlinien zur Versandautorisierung von Amazon SES kann der Principal entweder das AWS Konto Ihres Delegierten Absenders oder Ihr AWS Identity and Access Management (IAM-) Benutzer-ARN oder ein AWS Service sein.

Eine einfache Möglichkeit, dies zu bedenken, besteht darin, dass der Prinzipal (delegierter Sender) der Empfänger ist und Sie (Identitätsbesitzer) der Erteilender in der Autorisierungsrichtlinie sind, in der Sie ihm die Berechtigung zum Senden einer beliebigen Kombination aus E-Mail, Roh-E-Mail,

Vorlagen-E-Mail oder Massen-Vorlagen-E-Mail von der Ressource (bestätigte Identität) erlaubt, die Sie besitzen.

Wenn Sie über größtmögliche Kontrolle verfügen möchten, bitten Sie den delegierten Sender einen IAM-Benutzer einzurichten. Auf diese Weise kann nur ein delegierter Sender in Ihrem Namen E-Mails senden und nicht jeder Benutzer, der sich im AWS -Konto des delegierten Senders befindet. Der delegierte Sender kann unter Erstellen eines IAM-Benutzers in Ihrem AWS -Konto im IAM Benutzerhandbuch weitere Informationen über das Einrichten eines IAM-Benutzers finden.

Fragen Sie Ihren delegierten Absender nach der AWS Konto-ID oder dem Amazon-Ressourcennamen (ARN) des IAM-Benutzers, damit Sie ihn in Ihre Versandautorisierungsrichtlinie aufnehmen können. Sie können den stellvertretenden Sender an die Anweisungen zum Auffinden dieser Information unter Bereitstellen von Informationen für den Identitätsbesitzer verweisen. Wenn es sich bei dem Absender des Delegierten um einen AWS Dienst handelt, finden Sie den Namen des Dienstes in der Dokumentation zu diesem Dienst.

Die folgende Beispielrichtlinie veranschaulicht die grundlegenden Elemente dessen, was in einer Richtlinie erforderlich ist, die vom Identitätsbesitzer erstellt wurde, um den delegierten Sender zum Senden von der Ressource des Identitätsbesitzers zu autorisieren. Der Identitätsbesitzer würde in den Workflow „Verified identities“ (Verifizierte Identitäten) wechseln und unter Autorisierung den Richtliniengenerator verwenden, um in seiner einfachsten Form die folgende grundlegende Richtlinie zu erstellen, die es dem delegierten Sender ermöglicht, im Namen einer Ressource des Identitätsbesitzers zu senden:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSESSendEmail",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource": [
```

```
            "arn:aws:ses:us-east-1:444455556666:identity/bob@example.com"
        ],
        "Condition": {}
      }
    ]
}
```

Für die obige Richtlinie erläutert die folgende Legende die Schlüsselelemente und wem sie gehören:

- Prinzipal – dieses Feld wird mit dem ARN des IAM-Benutzers des delegierten Senders ausgefüllt.
- Aktion – Dieses Feld wird mit zwei SES-Aktionen (`SendEmail` und `SendRawEmail`) gefüllt, die der Identitätsbesitzer dem delegierten Sender von der Ressource des Identitätsbesitzers aus ausführen lässt.
- Ressource – Dieses Feld wird mit der verifizierten Ressource des Identitätsbesitzers ausgefüllt, von der er den delegierten Sender zum Senden autorisiert.

Erstellen einer Sendeautorisierungsrichtlinie in Amazon SES

Ähnlich wie beim Erstellen einer Autorisierungsrichtlinie in Amazon SES, wie unter Erstellen einer Identitätsautorisierungsrichtlinie beschrieben, erstellen Sie die Richtlinie unter Angabe von API-Aktionen zum Senden in SES und fügen diese Richtlinie dann der Identität an, um einen delegierten Sender zum Senden von E-Mails mit einer E-Mail-Adresse oder Domain (einer Identität) in Ihrem Besitz zu autorisieren.

Eine Liste der API-Aktionen, die in einer Sendeautorisierungsrichtlinie angegeben werden können, finden Sie in der Zeile Action in der Tabelle the section called “Richtlinienspezifische Anweisungen”.

Sie können eine Sendeautorisierungsrichtlinie erstellen, indem Sie entweder den Richtliniengenerator verwenden oder eine benutzerdefinierte Richtlinie erstellen. Es werden für beide Methoden der Erstellung einer Sendeautorisierungsrichtlinie spezifische Anleitungen bereitgestellt.

> **Note**
>
> - Sendeautorisierungsrichtlinien, die Sie an E-Mail-Adressidentitäten anfügen, haben Vorrang vor Richtlinien, die Sie den entsprechenden Domänenidentitäten anfügen. Wenn Sie beispielsweise eine Richtlinie für example.com erstellen, die einen delegierten Sender nicht zulässt, und eine Richtlinie für sender@example.com die den delegierten Sender

zulässt, kann der delegierte Sender E-Mails von sender@example.com senden, jedoch von keiner anderen Adresse in der Domäne example.com.

- Wenn Sie eine Richtlinie für example.com erstellen, die einen stellvertretenden Sender zulässt, und eine Richtlinie für sender@example.com, die den stellvertretenden Sender nicht zulässt, kann der stellvertretende Sender E-Mails von jeder Adresse in der Domäne example.com senden, mit Ausnahme von sender@example.com.
- Wenn Sie mit der Struktur von SES-Autorisierungsrichtlinien nicht vertraut sind, informieren Sie sich unter Richtlinienanatomie.
- Wenn die Identität, die Sie autorisieren, im Rahmen der Funktion Globale Endgeräte in einer sekundären Region dupliziert wird, müssen Sie Sendeautorisierungsrichtlinien für die Identität sowohl in der primären als auch in der sekundären Region erstellen, damit der delegierte Absender berechtigt ist, diese Identität für den Versand in beiden Regionen zu verwenden.

Erstellen einer Sendeautorisierungsrichtlinie mithilfe des Richtliniengenerators

Sie können den Richtliniengenerator verwenden, um eine Sendeautorisierungsrichtlinie zu erstellen, indem Sie diese Schritte ausführen.

So erstellen Sie eine Sendeautorisierungsrichtlinie mithilfe des Richtliniengenerators

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie im Container Identities (Identitäten) auf dem Bildschirm Verified identities (Verifizierte Identitäten) die verifizierte Identität aus, die Sie für den delegierten Sender autorisieren möchten, um sie in Ihrem Namen zu senden.
4. Wählen Sie die Registerkarte Autorisierung der verifizierten Identität aus.
5. Wählen Sie im Bereich Authorization policies (Autorisierungsrichtlinien) Create policy (Richtlinie erstellen) und anschließend in der Drop-down-Liste Use policy generator (Richtliniengenerator verwenden) aus.
6. Wählen Sie im Bereich Create statement (Anweisung erstellen) im Feld Effect (Effekt) die Option Allow (Erlauben) aus. (Wenn Sie eine Richtlinie erstellen möchten, um Ihren delegierten Sender einzuschränken, wählen Sie stattdessen Deny (Verweigern).)

7. Geben Sie im Feld Principals (Prinzipale) die AWS-Konto -ID oder den IAM user ARN (IAM-Benutzer-ARN) ein, die Ihr delegierter Sender mit Ihnen geteilt hat, um ihn zu autorisieren, E-Mails im Namen Ihres Kontos für diese Identität zu senden und wählen Sie dann Add (Hinzufügen) aus. (Wenn Sie mehr als einen delegierten Sender autorisieren möchten, wiederholen Sie diesen Schritt für jeden.)
8. Aktivieren Sie im Feld Actions (Aktionen) das Kontrollkästchen für jeden Sendetyp, den Sie für Ihren delegierten Sender autorisieren möchten.
9. (Optional) Erweitern Sie Specify conditions (Bedingungen angeben), wenn Sie der Berechtigung für den delegierten Sender eine qualifizierende Anweisung hinzufügen möchten.
    a. Wählen Sie einen Operator aus der Dropdown-Liste Operator aus.
    b. Wählen Sie einen Typ aus der Dropdown-Liste Key (Schlüssel) aus.
    c. Geben Sie den Wert des ausgewählten Schlüsseltyps in das Feld Value (Wert) ein. (Wenn Sie weitere Bedingungen hinzufügen möchten, wählen Sie Add new condition (Neue Bedingung hinzufügen) und wiederholen Sie diesen Schritt für jede weitere.)
10. Wählen Sie Save statement (Anweisung speichern) aus.
11. (Optional) Erweitern Sie Create another statement (Eine weitere Anweisung erstellen), wenn Sie Ihrer Richtlinie weitere Anweisungen hinzufügen möchten und wiederholen Sie die Schritte 6 - 10.
12. Wählen Sie Next (Weiter) und auf dem Bildschirm Cutomize policy (Richtlinie anpassen) enthält der Container Edit policy details (Richtliniendetails bearbeiten) Felder, in denen Sie Name der Richtlinie und das Policy document (Richtliniendokument) selbst ändern oder anpassen können.
13. Wählen Sie Next (Weiter) und auf dem Bildschirm Review and apply (Überprüfen und anwenden) zeigt der Container Overview (Übersicht) die bestätigte Identität an, die Sie für Ihren delegierten Sender autorisieren, sowie den Namen dieser Richtlinie. Im Bereich Policy document (Richtliniendokument) wird die aktuelle Richtlinie, die Sie gerade geschrieben haben, zusammen mit den von Ihnen hinzugefügten Bedingungen angezeigt. Überprüfen Sie die Richtlinie und wählen Sie Apply policy (Richtlinie anwenden), wenn sie richtig aussieht. (Wenn Sie etwas ändern oder korrigieren müssen, wählen Sie Previous (Zurück) und arbeiten Sie im Container Edit policy details (Richtliniendetails bearbeiten).) Die gerade erstellte Richtlinie ermöglicht es Ihrem delegierten Sender, in Ihrem Namen zu senden.
14. (Optional) Wenn Ihr delegierter Sender auch ein SNS-Thema verwenden möchte, das er besitzt, um Feedback-Benachrichtigungen zu erhalten, wenn er Unzustellbarkeit oder Beschwerden erhält oder wenn E-Mails zugestellt werden, müssen Sie sein SNS-Thema in dieser verifizierten

Identität konfigurieren. (Ihr delegierter Sender muss mit Ihnen seinen SNS-Thema-ARN teilen.) Wählen Sie die Registerkarte Notifications (Benachrichtigungen) und wählen Sie Edit (Bearbeiten) im Container Feedback notifications (Feedback-Benachrichtigungen):

a. Wählen Sie im Bereich SNS-Themen konfigurieren in einem der Feedbackfelder (Unzustellbarkeit, Beschwerde oder Zustellung) ein SNS-Thema aus, das Ihnen nicht gehört und geben Sie den SNS-Themen-ARN ein, der Ihnen gehört und von Ihrem delegierten Sender für Sie freigegeben wurde. (Nur Ihr delegierter Sender erhält diese Benachrichtigungen, da er das SNS-Thema besitzt – Sie als Identitätsbesitzer nicht.)

b. (Optional) Wenn Sie möchten, dass Ihre Themenachrichtigung die Header der ursprünglichen E-Mail einschließt, aktivieren Sie das Kontrollkästchen Einschließen von ursprünglichen E-Mail-Header direkt unter dem SNS-Themennamen jedes Feedback-Typs. Diese Option ist nur verfügbar, sofern Sie der zugeordneten Benachrichtigungsart ein Amazon-SNS-Thema zugewiesen haben. Weitere Informationen zum Inhalt der ursprünglichen E-Mail-Header finden Sie im Abschnitt zum `mail`-Objekt unter Benachrichtigungsinhalte.

c. Wählen Sie Änderungen speichern aus. Es kann ein paar Minuten dauern, bis die Änderungen an den Benachrichtigungseinstellungen übernommen werden.

d. (Optional) Da Ihr delegierter Sender Benachrichtigungen über Amazon-SNS-Themenbenachrichtigungen für Unzustellbarkeit und Beschwerden erhält, können Sie E-Mail-Benachrichtigungen vollständig deaktivieren, wenn Sie kein Feedback für die Sendungen dieser Identität erhalten möchten. Um E-Mail-Feedback für Unzustellbarkeiten und Beschwerden zu deaktivieren, wählen Sie auf der Registerkarte Notifications (Benachrichtigungen) im Container Email Feedback Forwarding (E-Mail-Feedback-Weiterleitung) die Option Edit (Bearbeiten), deaktivieren Sie das Kontrollkästchen Enabled (Aktiviert) und wählen Sie Save changes (Änderungen speichern). Benachrichtigungen über den Lieferstatus werden jetzt nur an die SNS-Themen gesendet, die Ihrem delegierten Sender gehören.

Erstellen einer benutzerdefinierten Sendeautorisierungsrichtlinie

Wenn Sie eine benutzerdefinierte Sendeautorisierungsrichtlinie erstellen und Sie einer Identität anfügen möchten, haben Sie die folgenden Optionen:

- Mithilfe der Amazon-SES-API – Erstellen Sie eine Richtlinie in einem Texteditor, und fügen Sie die Richtlinie dann mithilfe der in der Amazon-Simple-Email-Service-API-Referenz beschriebenen `PutIdentityPolicy`API an die Identität an.

- Mithilfe der Amazon-SES-Konsole – Erstellen Sie die Richtlinie in einem Texteditor und fügen Sie sie anschließend einer Identität hinzu, indem Sie die Richtlinie in den Editor für benutzerdefinierte Richtlinien in der Amazon-SES-Konsole einfügen. Im folgenden Abschnitt wird diese Methode beschrieben.

So erstellen Sie eine benutzerdefinierte Sendeautorisierungsrichtlinie mit dem Editor für benutzerdefinierte Richtlinien

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie im Container Identities (Identitäten) auf dem Bildschirm Verified identities (Verifizierte Identitäten) die verifizierte Identität aus, die Sie für den delegierten Sender autorisieren möchten, um sie in Ihrem Namen zu senden.
4. Wählen Sie im Detailfenster der verifizierten Identität, die Sie im vorherigen Schritt ausgewählt haben, die Registerkarte Authorization (Autorisierung).
5. Wählen Sie im Bereich Authorization policies (Autorisierungsrichtlinien) Create policy (Richtlinie erstellen) und anschließend in der Drop-down-Liste Create custom policy (Benutzerdefinierte Richtlinie erstellen) aus.
6. Geben oder fügen Sie im Bereich Policy document (Richtliniendokument) den Text Ihrer Richtlinie im JSON-Format ein. Sie können den Richtliniengenerator auch zum schnellen Erstellen der grundlegenden Struktur einer Richtlinie verwenden und diese anschließend hier anpassen.
7. Klicken Sie auf Apply Policy (Richtlinie anwenden). (Wenn Sie Ihre benutzerdefinierte Richtlinie jemals ändern müssen, aktivieren Sie einfach das Kontrollkästchen auf der Registerkarte Authorization (Autorisierung), wählen Sie Edit (Bearbeiten) und nehmen Sie Ihre Änderungen im Bereich Policy document (Richtliniendokument) vor und Save changes (Änderungen speichern) vor).
8. (Optional) Wenn Ihr delegierter Sender auch ein SNS-Thema verwenden möchte, das er besitzt, um Feedback-Benachrichtigungen zu erhalten, wenn er Unzustellbarkeit oder Beschwerden erhält oder wenn E-Mails zugestellt werden, müssen Sie sein SNS-Thema in dieser verifizierten Identität konfigurieren. (Ihr delegierter Sender muss mit Ihnen seinen SNS-Thema-ARN teilen.) Wählen Sie die Registerkarte Notifications (Benachrichtigungen) und wählen Sie Edit (Bearbeiten) im Container Feedback notifications (Feedback-Benachrichtigungen):

a. Wählen Sie im Bereich SNS-Themen konfigurieren in einem der Feedbackfelder (Unzustellbarkeit, Beschwerde oder Zustellung) ein SNS-Thema aus, das Ihnen nicht gehört und geben Sie den SNS-Themen-ARN ein, der Ihnen gehört und von Ihrem delegierten Sender für Sie freigegeben wurde. (Nur Ihr delegierter Sender erhält diese Benachrichtigungen, da er das SNS-Thema besitzt – Sie als Identitätsbesitzer nicht.)

b. (Optional) Wenn Sie möchten, dass Ihre Themenachrichtigung die Header der ursprünglichen E-Mail einschließt, aktivieren Sie das Kontrollkästchen Einschließen von ursprünglichen E-Mail-Header direkt unter dem SNS-Themennamen jedes Feedback-Typs. Diese Option ist nur verfügbar, sofern Sie der zugeordneten Benachrichtigungsart ein Amazon-SNS-Thema zugewiesen haben. Weitere Informationen zum Inhalt der ursprünglichen E-Mail-Header finden Sie im Abschnitt zum `mail`-Objekt unter Benachrichtigungsinhalte.

c. Wählen Sie Änderungen speichern aus. Es kann ein paar Minuten dauern, bis die Änderungen an den Benachrichtigungseinstellungen übernommen werden.

d. (Optional) Da Ihr delegierter Sender Benachrichtigungen über Amazon-SNS-Themenbenachrichtigungen für Unzustellbarkeit und Beschwerden erhält, können Sie E-Mail-Benachrichtigungen vollständig deaktivieren, wenn Sie kein Feedback für die Sendungen dieser Identität erhalten möchten. Um E-Mail-Feedback für Unzustellbarkeiten und Beschwerden zu deaktivieren, wählen Sie auf der Registerkarte Notifications (Benachrichtigungen) im Container Email Feedback Forwarding (E-Mail-Feedback-Weiterleitung) die Option Edit (Bearbeiten), deaktivieren Sie das Kontrollkästchen Enabled (Aktiviert) und wählen Sie Save changes (Änderungen speichern). Benachrichtigungen über den Lieferstatus werden jetzt nur an die SNS-Themen gesendet, die Ihrem delegierten Sender gehören.

Beispiele für Senderichtlinien

In der Sendeautorisierung können Sie die spezifischen Bedingungen angeben, unter denen stellvertretende Sender in Ihrem Namen E-Mails senden dürfen.

Die folgenden Bedingungen und Beispiele zeigen, wie Sie die Richtlinien erstellen müssen, um die verschiedenen Aspekte des Sendens zu kontrollieren:

- Spezifische Bedingungen für die Sendeautorisierung
- Angeben des delegierten Senders
- Beschränken der "From"-Adresse

- Beschränken der Zeit, zu der der delegierte Sender E-Mails senden kann
- Beschränkung des E-Mail-Versands
- Beschränken des Anzeigenamens des E-Mail-Senders
- Verwenden mehrerer Anweisungen

Spezifische Bedingungen für die Sendeautorisierung

Bei einer Bedingung handelt es sich um jegliche Einschränkung, die die Berechtigung in der Anweisung betrifft. Der Teil der Anweisung, der die Bedingungen festlegt, kann der ausführlichste aller Bestandteile sein. Ein Schlüssel ist die Besonderheit, die die Grundlage für die Zugriffsbeschränkung, z. B. das Datum und die Uhrzeit der Anfrage, darstellt.

Sie verwenden Bedingungen und Schlüssel zusammen, um die Einschränkung auszudrücken. Wenn Sie beispielsweise den stellvertretenden Sender davon abhalten möchten, nach dem 30. Juli 2019 in Ihrem Namen Anfragen an Amazon SES zu stellen, verwenden Sie die Bedingung namens `DateLessThan`. Sie verwenden den Schlüssel `aws:CurrentTime` und legen den Wert mit `2019-07-30T00:00:00Z` fest.

Sie können einen der AWS-weiten Schlüssel verwenden, die im IAM-Benutzerhandbuch unter Verfügbare Schlüssel aufgeführt sind, oder Sie können einen der folgenden SES-spezifischen Schlüssel verwenden, die beim Senden von Autorisierungsrichtlinien nützlich sind:

Bedingungsschlüssel	Description
`ses:Recipients`	Beschränkt die Empfängeradressen, einschließlich der Adressen "To", "CC" und "BCC".
`ses:FromAddress`	Beschränkt die "From"-Adresse.
`ses:FromDisplayName`	Beschränkt den Inhalt der Zeichenfolge, die als der "From"-Anzeigename verwendet wird (manchmal auch "Friendly from" genannt). So lautet beispielsweise der Anzeigename für "John Doe <johndoe@example.com>" John Doe.
`ses:FeedbackAddress`	Beschränkt die "Return Path"-Adresse. Dies ist die Adresse, an die Unzustellbarkeitsnachrichten und Beschwerden an Sie anhand von Feedback-E-Mails

Bedingungsschlüssel	Description
	weitergeleitet werden können. Weitere Informationen zum Weiterleiten von Feedback per E-Mail finden Sie unter Verwenden von Benachrichtigungen für den Amazon-SES-E-Mail-Empfang.

Sie können die Bedingungen `StringEquals` und `StringLike` mit Amazon-SES-Schlüsseln verwenden. Für diese Bedingungen wird zur Übereinstimmung der Zeichenfolge die Groß-/Kleinschreibung beachtet. Für `StringLike` können die Werte einen Mehrzeichenplatzhalter (*) oder einen Einzelzeichenplatzhalter (?) an einer beliebigen Stelle in der Zeichenfolge enthalten. Die folgende Bedingung gibt beispielsweise an, dass der stellvertretende Sender nur von einer "From" -Adresse senden kann, die mit der Fakturierung beginnt und mit @example.comendet:

```
"Condition": {
    "StringLike": {
      "ses:FromAddress": "invoicing*@example.com"
    }
}
```

Sie können auch die Bedingung `StringNotLike` verwenden, um zu verhindern, dass stellvertretende Sender E-Mails von bestimmten E-Mail-Adressen senden. Beispielsweise können Sie das Senden von E-Mails von admin@example.com sowie von ähnlichen Adressen wie "admin"@example.com, admin+1@example.com oder sender@admin.example.com untersagen, indem Sie die folgende Bedingung in Ihre Richtlinienanweisung aufnehmen:

```
"Condition": {
    "StringNotLike": {
      "ses:FromAddress": "*admin*example.com"
    }
 }
```

Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema IAM;-JSON-Richtlinienelemente: Bedingung im IAM Benutzerhandbuch.

Angeben des delegierten Senders

Der Principal, also die Entität, der Sie die Erlaubnis erteilen, kann ein AWS-Konto AWS Identity and Access Management (IAM-) Benutzer oder ein Dienst sein. AWS

Das folgende Beispiel zeigt eine einfache Richtlinie, die es der AWS ID 123456789012 ermöglicht, E-Mails von der verifizierten Identität example.com (die 888888888888 gehört) zu senden. AWS-Konto Die *`Condition`* Aussage in dieser Richtlinie erlaubt nur dem Delegierten (d. h. der ID 123456789012), E-Mails von der Adresse marketing+ zu senden AWS . * @example .com, wobei * eine beliebige Zeichenfolge ist, die der Absender nach marketing+ hinzufügen möchte. .

JSON

```
{
  "Id":"SampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeMarketer",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringLike":{
          "ses:FromAddress":"marketing+.*@example.com"
        }
      }
    }
  ]
}
```

Die folgende Beispielrichtlinie erteilt zwei IAM-Benutzern die Berechtigung, von der Identität example.com E-Mails zu senden. Die IAM-Benutzer werden durch ihren Amazon-Ressourcennamen (ARN) angegeben.

JSON

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeIAMUser",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::111122223333:user/John",
          "arn:aws:iam::444455556666:user/Jane"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ]
    }
  ]
}
```

Die folgende Beispielrichtlinie erteilt Amazon Cognito die Berechtigung, von der Identität example.com E-Mails zu senden.

JSON

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeService",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "Service":[
          "cognito-idp.amazonaws.com"
```

```
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "888888888888",
          "aws:SourceArn": "arn:aws:cognito-idp:us-east-1:888888888888:userpool/
your-user-pool-id-goes-here"
        }
      }
    }
  ]
}
```

Die folgende Beispielrichtlinie erteilt allen Konten innerhalb einer AWS Organization die Berechtigung zum Senden von Identitäts- example.com. Die AWS Organisation wird mithilfe des globalen Bedingungsschlüssels PrincipalOrgID angegeben.

JSON

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeOrg",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":"*",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":"o-xxxxxxxxxx"
        }
      }
```

```
    }
  ]
}
```

Beschränken der "From"-Adresse

Wenn Sie eine verifizierte Domäne verwenden, können Sie eine Richtlinie erstellen, die dem delegierten Sender nur ermöglicht, E-Mails von einer bestimmten E-Mail-Adresse zu senden. Um die Absenderadresse einzuschränken, legen Sie für den Schlüssel eine Bedingung namens ses:festFromAddress. Die folgende Richtlinie ermöglicht das Senden der AWS-Konto ID 123456789012 von der Identität example.com aus, jedoch nur von der E-Mail-Adresse sender@example.com.

JSON

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeFromAddress",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"sender@example.com"
        }
      }
    }
  ]
}
```

Beschränken der Zeit, zu der der delegierte Sender E-Mails senden kann

Sie können die Senderautorisierungsrichtlinie auch so konfigurieren, dass ein stellvertretender Sender E-Mails nur zu einer bestimmten Tageszeit oder während eines bestimmten Zeitraums senden kann. Wenn Sie beispielsweise im September 2021 eine E-Mail-Kampagne planen, können Sie mit der folgenden Richtlinie die Möglichkeit des delegierten Senders, E-Mails zu versenden, auf diesen Monat beschränken.

JSON

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"ControlTimePeriod",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "DateGreaterThan":{
          "aws:CurrentTime":"2021-08-31T12:00Z"
        },
        "DateLessThan":{
          "aws:CurrentTime":"2021-10-01T12:00Z"
        }
      }
    }
  ]
}
```

Beschränkung des E-Mail-Versands

Sender können zwei Aktionen verwenden, um eine E-Mail mit Amazon SES zu senden: `SendEmail` und `SendRawEmail`, je nachdem, wie viel Kontrolle der Sender über das Format der E-Mail haben möchte. Anhand von Sendeautorisierungsrichtlinien können Sie den stellvertretenden Sender auf eine dieser beiden Aktionen beschränken. Jedoch überlassen viele Identitätsbesitzer die Details der Aufrufe zum Senden der E-Mails dem stellvertretenden Sender, indem sie beide Aktionen in ihren Richtlinien aktivieren.

> **Note**
>
> Soll der stellvertretende Sender in der Lage sein, über die SMTP-Schnittstelle auf Amazon SES zugreifen zu können, müssen Sie zumindest `SendRawEmail` auswählen.

Wenn Sie für Ihren Anwendungsfall die Aktion einschränken möchten, schließen Sie nur eine der Aktionen in die Sendeautorisierungsrichtlinie ein. Das folgende Beispiel zeigt, wie Sie die Aktion auf `SendRawEmail` beschränken.

JSON

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"ControlAction",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendRawEmail"
      ]
    }
  ]
}
```

Beschränken des Anzeigenamens des E-Mail-Senders

Einige E-Mail-Clients zeigen den "friendly"-Namen des E-Mail-Senders (sofern die E-Mail-Kopfzeile dies unterstützt) und nicht die tatsächliche "From"-Adresse an. So lautet beispielsweise der Anzeigename für "John Doe <johndoe@example.com>" John Doe. Wenn Sie beispielsweise E-Mails von user@example.com senden, es aber bevorzugen, dass die Empfänger Marketing und nicht user@example.com als den Sender der E-Mail sehen. Mit der folgenden Richtlinie kann die AWS-Konto ID 123456789012 von identity example.com aus gesendet werden, jedoch nur, wenn der Anzeigename der Absenderadresse Marketing enthält.

JSON

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeFromAddress",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringLike":{
          "ses:FromDisplayName":"Marketing"
        }
      }
    }
  ]
}
```

Verwenden mehrerer Anweisungen

Ihre Sendeautorisierungsrichtlinie kann mehrere Anweisungen enthalten. Die folgende Beispielrichtlinie enthält zwei Anweisungen. Die erste Anweisung autorisiert zwei Personen, von sender@example.com aus AWS-Konten zu senden, sofern sowohl die Absenderadresse als auch die Feedback-Adresse die Domain example.com verwenden. Die zweite Anweisung autorisiert einen IAM-Benutzer, E-Mails von sender@example.com zu senden, solange sich die E-Mail-Adresse des Empfängers unter der Domäne example.com befindet.

Bereitstellen der Identitätsinformationen für den delegierten Sender im Zusammenhang mit der Amazon-SES-Sendeautorisierung

Nachdem Sie die Richtlinie für die Sendeautorisierung erstellt und sie Ihrer Identität angefügt haben, können Sie dem stellvertretenden Sender den Amazon-Ressourcennamen (ARN) der Identität mitteilen. Der stellvertretende Sender übergibt den ARN während des Sendevorgangs oder in der Kopfzeile der E-Mail an Amazon SES. Um den ARN Ihrer Identität zu finden, führen Sie diese Schritte aus.

So finden Sie den ARN einer Identität

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Verified identities (Verifizierte Identitäten) aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, der Sie die Sendeautorisierungsrichtlinie angefügt haben.
4. Im Bereich Summary (Zusammenfassung) enthält die zweite Spalte, Amazon-Ressourcenname (ARN), den ARN der Identität. Er sollte folgendem Beispiel ähneln: arn:aws:ses:us-east-1:123456789012:identity/user@example.com. Kopieren Sie den gesamte ARN und geben Sie ihn dem stellvertretenden Sender.

> **Important**
>
> Wenn die Identität, die Sie autorisieren, im Rahmen der Funktion „Globale Endgeräte“ in einer sekundären Region dupliziert wird, ersetzen Sie den Regionsparameter, z. B.,`us-east-1`, durch ein Sternchen `*` wie im folgenden Beispiel.
> `arn:aws:ses:*:123456789012:identity/user@example.com`

Delegieren der Senderaufgaben für die Amazon-SES-Sendeautorisierung

Als delegierter Sender senden Sie E-Mails im Namen einer Identität, die Ihnen nicht gehört, zu deren Verwendung Sie jedoch berechtigt sind. Auch wenn Sie im Namen des Identitätsinhabers versenden, werden Bounces und Beschwerden auf die Metriken zu Bounce und Beschwerden für Ihr AWS Konto angerechnet, und die Anzahl der von Ihnen gesendeten Nachrichten wird auf Ihr Versandkontingent angerechnet. Sie sind auch dafür verantwortlich, wenn Sie eine Erhöhung der Sendequote anfordern, um die E-Mails des Identitätsbesitzers zu versenden.

Als stellvertretender Sender müssen Sie die folgenden Aufgaben ausführen:

- Bereitstellen von Informationen für den Identitätsbesitzer
- Benachrichtigungen an den delegierten Sender
- Senden von E-Mails im Namen des Identitätsbesitzers

Bereitstellen von Informationen für den Identitätsbesitzer im Zusammenhang mit der Amazon-SES-Sendeautorisierung

Als delegierter Absender müssen Sie dem Identitätsinhaber entweder Ihre AWS Konto-ID oder den Amazon Resource Name (ARN) Ihres IAM-Benutzers mitteilen, da Sie E-Mails im Namen des Identitätsinhabers senden. Der Identitätsinhaber benötigt Ihre Kontoinformationen, damit er eine Richtlinie erstellen kann, die Ihnen die Erlaubnis erteilt, von einer seiner verifizierten Identitäten aus zu senden.

Wenn Sie Ihre eigenen SNS-Themen verwenden möchten, können Sie beantragen, dass Ihr Identitätsbesitzer Feedback-Benachrichtigungen für Unzustellbarkeiten, Beschwerden oder Lieferungen konfiguriert, die an eines oder mehrere Ihrer SNS-Themen gesendet werden. Dazu musst du deinen SNS-Thema-ARN mit deinem Identitätsinhaber teilen, damit dieser dein SNS-Thema in der verifizierten Identität konfigurieren kann, von der aus er dich zum Senden autorisiert hat.

In den folgenden Verfahren wird erklärt, wie Sie Ihre Kontoinformationen und Ihr SNS-Thema finden, um sie mit Ihrem ARNs Identitätsinhaber zu teilen.

So finden Sie Ihre AWS Konto-ID

1. Melden Sie sich unter AWS-Managementkonsole an https://console.aws.amazon.com.
2. Erweitern Sie in der oberen rechten Ecke der Konsole Ihre name/account Nummer und wählen Sie in der Dropdownliste Mein Konto aus.

3. Die Seite mit den Kontoeinstellungen wird geöffnet und zeigt all Ihre Kontoinformationen, einschließlich Ihrer AWS Konto-ID, an.

So finden Sie Ihren ARN Ihres IAM-Benutzers

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich auf Users (Benutzer).
3. Wählen Sie in der Liste der Benutzer den Namen des Benutzers aus. Im Abschnitt Summary (Zusammenfassung) wird der IAM-Benutzer-ARN angezeigt. Der ARN sieht in etwa wie folgendes Beispiel aus: arn:aws:iam::123456789012:user/John.

So finden Sie Ihren SNS-Thema-ARN

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Themen aus.
3. In der Themenliste ARNs werden die SNS-Themen in der ARN-Spalte angezeigt. Der ARN ähnelt dem folgenden Beispiel: arn:aws:sns:us-east - 1:444455556666:. my-sns-topic

Benachrichtigungen an den delegierten Sender bei Verwendung der Amazon-SES-Sendeautorisierung

Als delegierter Sender senden Sie E-Mails im Namen einer Identität, die Ihnen nicht gehört, zu deren Verwendung Sie jedoch berechtigt sind. Unzustellbarkeiten und Beschwerden zählen jedoch weiterhin zu Ihren Unzustellbarkeits- und Beschwerde-Metriken, nicht denen des Identitätsbesitzers.

Wenn die Unzustellbarkeits- oder Beschwerderate für Ihr Konto zu hoch wird, besteht die Gefahr, dass Ihr Konto überprüft wird oder die Möglichkeit zum Senden von E-Mails angehalten wird. Aus diesem Grund ist es wichtig, dass Sie die Benachrichtigungen eingerichtet haben und über einen Prozess verfügen, mit dem sie überwacht werden können. Sie benötigen außerdem einen Prozess zum Entfernen von Adressen, die unzustellbar sind oder die sich beschwert haben, aus Ihrer Mailing-Listen.

Daher können Sie als delegierter Sender Amazon SES so konfigurieren, dass es Benachrichtigungen sendet, wenn Unzustellbarkeits- und Beschwerdeereignisse für die E-Mails auftreten, die Sie im Namen von Identitäten senden, die Sie nicht besitzen, aber vom Identitätsbesitzer zur Verwendung autorisiert wurden. Sie können auch die Veröffentlichung von Veranstaltungen einrichten, um

Benachrichtigungen über Abmeldungen und Beschwerden auf Amazon SNS oder Firehose zu veröffentlichen.

> **Note**
>
> Wenn Sie Amazon SES zum Senden von Benachrichtigungen über einrichten, werden Ihnen die üblichen Amazon-SNS-Standardgebühren für die Benachrichtigungen, die Sie erhalten, berechnet. Weitere Informationen finden Sie in der Amazon-SNS-Preisliste.

Erstellen einer neuen Benachrichtigung für den delegierten Sender

Sie können das delegierte Senden von Benachrichtigungen entweder mit Konfigurationssätzen unter Verwendung der Ereignisveröffentlichung oder mit verifizierten Identitäten einrichten, die mit Ihren eigenen SNS-Themen konfiguriert wurden.

Im Folgenden werden Verfahren zum Einrichten des delegierten Sendens von Benachrichtigungen mit einer der beiden Methoden beschrieben:

- Ereignisveröffentlichung über einen Konfigurationssatz
- Feedback-Benachrichtigungen zu SNS-Themen, die Sie besitzen

So richten Sie die Ereignisveröffentlichung über einen Konfigurationssatz für das delegierte Senden ein

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Folgen Sie den Verfahren in Ereignisziele erstellen.
3. Nachdem Sie die Ereignisveröffentlichung in Ihrem Konfigurationssatz eingerichtet haben, geben Sie den Namen des Konfigurationssatzes an, wenn Sie als delegierter Sender E-Mails mit der bestätigten Identität senden, von der der Identitätsbesitzer Sie autorisiert hat. Siehe Senden von E-Mails im Namen des Identitätsbesitzers.

So richten Sie Feedbackbenachrichtigungen zu SNS-Themen, deren Eigentümer Sie sind, für das delegierte Senden ein

1. Nachdem Sie sich entschieden haben, welches Ihrer SNS-Themen Sie für Feedbackbenachrichtigungen verwenden möchten, befolgen Sie die Schritte, um Ihren SNS-

Themen-ARN zu finden, kopieren Sie den vollständigen ARN und teilen Sie ihn mit Ihrem Identitätsbesitzer.

2. Bitten Sie Ihren Identitätsbesitzer, Ihre SNS-Themen für Feedback-Benachrichtigungen über die gemeinsame Identität zu konfigurieren, von der er Sie senden darf. (Ihr Identitätsbesitzer muss die Verfahren zum Konfigurieren von SNS-Themen in den Verfahren für die Autorisierungsrichtlinie befolgen.)

Senden von E-Mails im Namen des Identitätsbesitzers im Zusammenhang mit der Amazon-SES-Sendeautorisierung

Als delegierter Sender senden Sie E-Mails wie jeder andere Amazon-SES-Sender auch, mit der Ausnahme, dass Sie den Amazon-Ressourcennamen (ARN) der Identität angeben, für deren Nutzung Sie vom Identitätsbesitzer berechtigt wurden. Wenn Sie Amazon SES zum Senden der E-Mail aufrufen, überprüft Amazon SES, ob die von Ihnen angegebene Identität über eine Richtlinie verfügt, die Sie zum Senden der E-Mail berechtigt.

Es gibt verschiedene Möglichkeiten, wie Sie den ARN der Identität beim Senden einer E-Mail angeben können. Die zu verwendende Methode hängt davon ab, ob Sie sich für die Amazon-SES-API-Operationen oder die Amazon-SES-SMTP-Schnittstelle entscheiden.

Important

- Um erfolgreich eine E-Mail zu senden, müssen Sie eine Verbindung zum Amazon SES SES-Endpunkt in der AWS Region herstellen, in der der Identitätsinhaber die Identität verifiziert hat.
- Darüber hinaus müssen die AWS Konten sowohl des Identitätsinhabers als auch des delegierten Absenders aus der Sandbox entfernt werden, bevor eines der Konten E-Mails an nicht verifizierte Adressen senden kann. Weitere Informationen finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).
- Wenn die Identität, zu deren Verwendung Sie autorisiert wurden, im Rahmen der Funktion „Globale Endgeräte“ in einer sekundären Region dupliziert wird:
  - Der Identitätseigentümer hätte Ihnen einen Identitäts-ARN zur Verfügung stellen müssen, bei dem der Parameter Region`us-east-1`, `*` wie im folgenden Beispiel, `arn:aws:ses:*:123456789012:identity/user@example.com` durch ein Sternchen ersetzt wurde.

- Der Identitätsinhaber hätte für Sie Richtlinien zur Versandautorisierung sowohl in der primären als auch in der sekundären Region erstellen müssen.

Verwenden der Amazon-SES-API

Wie bei jedem Amazon SES-E-Mail-Absender können Sie, wenn Sie über die Amazon SES-API auf Amazon SES zugreifen (entweder direkt über HTTPS oder indirekt über ein AWS SDK), zwischen drei E-Mail-Versandaktionen wählen: `SendEmail`, `SendTemplatedEmail`, und. `SendRawEmail` Die Amazon Simple Email Service API-Referenz beschreibt deren Einzelheiten APIs, aber wir bieten hier einen Überblick über die Versandautorisierungsparameter.

SendRawEmail

Wenn Sie `SendRawEmail` verwenden möchten, um das Format Ihrer E-Mails kontrollieren zu können, können Sie die delegierte autorisierte Identität auf eine von zwei Arten festlegen:

- Übermitteln Sie optionale Parameter an die **`SendRawEmail`**-API. Die erforderlichen Parameter werden in der folgenden Tabelle beschrieben:

Parameter	Description
`SourceArn`	ARN der Identität, die mit der Sendeautorisierung srichtlinie verknüpft ist, die Sie zum Senden von E-Mail im Namen der im `Source`-Parameter von `SendRawEmail` angegebenen E-Mail-Adresse berechtigt. **Note** Wenn Sie nur den `SourceArn` angeben, legt Amazon SES für die Adressen „Von“ und „Rücksendepfad“ die Identität fest, die Sie im `SourceArn` festgelegt haben.
`FromArn`	ARN der Identität, die mit der Sendeautorisierung srichtlinie verknüpft ist, die Sie zur Angabe einer

Parameter	Description
	bestimmten "From"-Adresse im Header der Raw-E-Mail-Adresse berechtigt.
`ReturnPathArn`	ARN der Identität, die mit der Sendeautorisierung srichtlinie verknüpft ist, die Sie zum Verwenden der im `ReturnPath` -Parameter von `SendRawEmail` angegebenen E-Mail-Adresse berechtigt.

- Schließen Sie X-Header in die E-Mail ein. X-Header sind benutzerdefinierte Header, die Sie zusätzlich zu den Standard-E-Mail-Headern (wie „Von“, „Antworten“ oder „Betreff“) verwenden können. Amazon SES erkennt drei X-Header, die Sie zum Einrichten der Sendeautorisierungsparameter verwenden können:

> **Important**
>
> Schließen Sie diese X-Header nicht in der DKIM-Signatur mit ein, da sie vor dem Senden der E-Mail von Amazon SES entfernt werden.

X-Header	Description
`X-SES-SOURCE-ARN`	Entspricht dem `SourceArn` .
`X-SES-FROM-ARN`	Entspricht dem `FromArn`.
`X-SES-RETURN-PATH-ARN`	Entspricht dem `ReturnPathArn` .

Amazon SES entfernt alle X-Header vor dem Senden der E-Mail. Wenn Sie mehrere Instances eines X-Headers angeben, verwendet Amazon SES nur die erste Instance.

Das folgende Beispiel zeigt eine E-Mail, die für die Sendeautorisierung X-Header umfasst:

```
X-SES-SOURCE-ARN: arn:aws:ses:us-east-1:123456789012:identity/example.com
X-SES-FROM-ARN: arn:aws:ses:us-east-1:123456789012:identity/example.com
X-SES-RETURN-PATH-ARN: arn:aws:ses:us-east-1:123456789012:identity/example.com
```

```
From: sender@example.com
To: recipient@example.com
Return-Path: feedback@example.com
Subject: subject
Content-Type: multipart/alternative;
 boundary="----=_boundary"

------=_boundary
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

body
------=_boundary
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

body
------=_boundary--
```

SendEmail und SendTemplatedEmail

Wenn Sie die Operation `SendEmail` oder `SendTemplatedEmail` verwenden, können Sie die delegierte autorisierte Identität angeben, indem Sie die optionalen Parameter unten übergeben. Für die Methode `SendEmail` oder `SendTemplatedEmail` können Sie nicht die X-Header-Methode verwenden.

Parameter	Description
`SourceArn`	ARN der Identität, die mit der Sendeautorisierung srichtlinie verknüpft ist, die Sie zum Senden von E-Mail im Namen der im `Source`-Parameter entweder von `SendEmail` oder `SendTemplatedEmail` angegebenen E-Mail-Adresse berechtigt.
`ReturnPathArn`	ARN der Identität, die mit der Sendeautorisierung srichtlinie verknüpft ist, die Sie zum Verwenden der im `ReturnPath` -Parameter entweder von `SendEmail` oder `SendTemplatedEmail` angegebenen E-Mail-Adresse berechtigt.

Das folgende Beispiel zeigt, wie Sie eine E-Mail mit den Attributen `SourceArn` und `ReturnPathArn` unter Verwendung der Operation `SendEmail` oder `SendTemplatedEmail` und der SDK für Python senden.

```
import boto3
from botocore.exceptions import ClientError

# Create a new SES resource and specify a region.
client = boto3.client('ses',region_name="us-east-1")

# Try to send the email.
try:
    #Provide the contents of the email.
    response = client.send_email(
        Destination={
            'ToAddresses': [
                'recipient@example.com',
            ],
        },
        Message={
            'Body': {
                'Html': {
                    'Charset': 'UTF-8',
                    'Data': 'This email was sent with Amazon SES.',
                },
            },
            'Subject': {
                'Charset': 'UTF-8',
                'Data': 'Amazon SES Test',
            },
        },
        SourceArn='arn:aws:ses:us-east-1:123456789012:identity/example.com',
        ReturnPathArn='arn:aws:ses:us-east-1:123456789012:identity/example.com',
        Source='sender@example.com',
        ReturnPath='feedback@example.com'
    )
# Display an error if something goes wrong.
except ClientError as e:
    print(e.response['Error']['Message'])
else:
    print("Email sent! Message ID:"),
    print(response['ResponseMetadata']['RequestId'])
```

Verwenden der Amazon SES SMTP-Schnittstelle

Wenn Sie die SMTP-Schnittstelle von Amazon SES zum delegierten Senden verwenden, müssen Sie die Header `X-SES-SOURCE-ARN`, `X-SES-FROM-ARN` und `X-SES-RETURN-PATH-ARN` in Ihre Nachricht einfügen. Übergeben Sie diese Header, nachdem Sie den `DATA`-Befehl in der SMTP-Aushandlung erteilen.

Senden von Test-E-Mails in Amazon SES mit dem Simulator

Wir empfehlen, die Amazon-SES-Konsole zu verwenden, um eine Test-E-Mail mit Amazon SES zu senden. Da die Konsole die manuelle Eingabe von Informationen erfordert, verwenden Sie diese in der Regel nur zum Versenden von Test-E-Mails. Nach Ihren ersten Schritten mit werden Sie Ihre E-Mails wahrscheinlich entweder über die Amazon-SES-SMTP-Schnittstelle oder API versenden. Die Konsole ist jedoch praktisch, um Ihre Sendeaktivität zu überwachen. Die Konsole ist jedoch praktisch, um Ihre Sendeaktivität zu überwachen.

Die folgenden Themen erklären, wie Sie den Postfachsimulator sowohl von der -Konsole als auch manuell durch Senden einer E-Mail verwenden:

- Verwenden des Postfachsimulators über die Konsole
- Manuelles Verwenden des Postfachsimulators

Verwenden des Postfachsimulators über die Konsole

> **Important**
>
> - In diesem Tutorial senden Sie eine E-Mail von der Konsole aus an sich selbst, um zu prüfen, ob diese bei Ihnen ankommt. Weitere Experimente oder Lasttests finden Sie unter Manuelles Verwenden des Postfachsimulators.
> - E-Mails, die Sie an den Postfachsimulator senden, zählen nicht zu Ihrer Sendekontingent oder Ihre Unzustellbarkeits- und Beschwerderaten noch wirken sie sich auf die Metriken des virtuellen Zustellbarkeitsmanagers aus.

Bevor Sie diese Anweisungen befolgen, führen Sie die Schritte unter Amazon Simple Email Service einrichten aus.

So senden Sie eine Test-E-Mail-Nachricht aus der Amazon-SES-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Konfiguration die Option Identitäten aus.
3. Wählen Sie aus der Tabelle Identitäten eine verifizierte E-Mail-Identität aus (indem Sie direkt auf den Identitätsnamen klicken, anstatt das Kontrollkästchen zu aktivieren). Falls Sie keine verifizierte E-Mail-Identität haben, siehe Erstellen einer E-Mail-Adressidentität.
4. Wählen Sie auf der Detailseite der ausgewählten E-Mail-Identität Senden einer Test-E-Mail aus.
5. FürDetails zur Nachricht, wählen Sie dieE-Mail-Formataus. Folgende beiden Optionen sind verfügbar:

   - Formatted – Dies ist die einfachste Option. Wählen Sie diese Option, wenn Sie einfach nur den Text Ihrer Nachricht in das Textfeld Body eingeben möchten. Wenn Sie die E-Mail senden, setzt Amazon SES den Text für Sie in das E-Mail-Format um.
   - Raw – Wählen Sie diese Option, wenn Sie eine komplexere Nachricht senden möchten, z. B. eine Nachricht mit HTML oder einer Anlage. Aufgrund dieser Flexibilität müssen Sie die Nachricht selbst formatieren (wie unter Senden von Roh-E-Mails mit der Amazon SES API v2 beschrieben). Sie müssen dann die gesamte formatierte Nachricht einschließlich der Header in das Textfeld Body einfügen. Sie können das folgende Beispiel mit HTML verwenden, um eine Test-E-Mail mit dem Raw-E-Mail-Format zu versenden. Kopieren Sie diese Nachricht komplett in das Body-Textfeld. Vergewissern Sie sich, dass zwischen dem `MIME-Version`-Header und dem `Content-Type`-Header keine Leerzeile steht. Eine Leerzeile zwischen diesen beiden Zeilen bewirkt, dass die E-Mail anstelle von HTML als einfacher Text formatiert wird.

```
Subject: Amazon SES Raw Email Test
MIME-Version: 1.0
Content-Type: text/html

<!DOCTYPE html>
<html>
<body>
<h1>This text should be large, because it is formatted as a header in HTML.</h1>
<p>Here is a formatted link: <a href="https://docs.aws.amazon.com/ses/latest/
DeveloperGuide/Welcome.html">Amazon Simple Email Service Developer Guide</a>.</p>
</body>
</html>
```

6. Wählen Sie den Typ des simulierten E-Mail-Szenarios aus, das Sie testen möchten, indem Sie das Listenfeld Szenario wählen.

   - Wenn Sie Benutzerdefiniert wählen und noch immer in der Amazon-SES-Sandbox sind, stellen Sie sicher, dass die Adresse im Benutzerdefinierter Empfänger-Feld eine verifizierte E-Mail-Adresse ist. Weitere Informationen finden Sie unter Erstellen einer E-Mail-Adressidentität.

7. Füllen Sie die restlichen Felder wie gewünscht aus.
8. Wählen Sie Send Test Email (Test-E-Mail senden) aus.
9. Melden Sie sich beim E-Mail-Client der Adresse an, an die Sie die E-Mail gesendet haben. Sie finden die Nachricht, die Sie gesendet haben.

Manuelles Verwenden des Postfachsimulators

Amazon SES umfasst einen Postfachsimulator, den Sie verwenden können, um zu testen, wie Ihre Anwendung verschiedene E-Mail-Versandszenarien verarbeitet. Der Postfachsimulator ist nützlich, wenn Sie beispielsweise ein E-Mail-Programm testen möchten, ohne fiktive E-Mail-Adressen zu erstellen, oder wenn Sie den maximalen Durchsatz Ihres Systems ermitteln möchten, ohne Ihre tägliche Sendequote zu belasten.

Wichtige Überlegungen

Berücksichtigen Sie die folgenden Funktionen und Einschränkungen, wenn Sie den Amazon-SES-Postfachsimulator verwenden:

- Sie können den Postfachsimulator auch verwenden, wenn Ihr Konto sich in der Amazon-SES-Sandbox-Umgebung befindet.
- E-Mails, die Sie an den Postfachsimulator senden, werden auf die maximale Senderate Ihres Kontos beschränkt, aber sie wirken sich nicht auf Ihr tägliches Sendekontingent aus. Beispiel: Wenn Ihr Konto zum Senden von 10 000 Nachrichten je 24-Stunden-Zeitraum autorisiert ist und Sie 100 Nachrichten an den Postfachsimulator senden, können Sie dennoch bis zu 10.000 Nachrichten an reguläre Empfänger senden, ohne die Grenze Ihres Sendekontingents zu erreichen.
- E-Mails, die Sie an den Postfachsimulator senden, haben keine Auswirkung auf Ihre E-Mail-Zustellbarkeits- oder Zuverlässigkeitsmetriken. Beispiel: Wenn Sie eine große Anzahl von Nachrichten an die Unzustellbarkeits-Adresse des E-Mail-Simulators senden, führt dies nicht dazu,

dass das Zuverlässigkeits-Dashboard eine Warnung anzeigt, dass Ihre Unzustellbarkeitsquote zu hoch ist.

- Zu Fakturierungszwecken sind E-Mails, die Sie an den Amazon-SES-Postfachsimulator senden, die gleichen wie bei jeder anderen E-Mail, die Sie mithilfe von Amazon SES versenden. Mit anderen Worten, wir stellen Ihnen für Nachrichten, die Sie an den Postfachsimulator senden, den gleichen Betrag in Rechnung wie für Nachrichten, die Sie an reguläre Empfänger senden.
- Der Postfachsimulator unterstützt die Kennzeichnung, sodass Sie E-Mails auf unterschiedliche Weise an dieselbe Adresse des Postfachsimulators senden oder sehen können, wie Ihre Anwendung VERP (Variable Envelope Return Path) verarbeitet. Beispielsweise können Sie eine E-Mail an die Adresse bounce+label1@simulator.amazonses.com und bounce +label2@simulator.amazonses.com senden, um zu sehen, ob Ihre Anwendung eine Unzustellbarkeitsnachricht der E-Mail-Adresse zuordnen kann, die diese Unzustellbarkeit verursacht hat.
- Wenn Sie den Postfachsimulator zur Simulation mehrerer Unzustellbarkeitsnachrichten derselben Sendeanforderung verwenden, kombiniert Amazon SES die Unzustellbarkeitsantworten in einer einzigen Antwortnachricht.

Verwenden des Postfachsimulators

Um den E-Mail-Simulator zu verwenden, suchen Sie das Szenario in der folgenden Tabelle, und senden Sie dann eine E-Mail an die entsprechende E-Mail-Adresse.

> **Note**
>
> Wenn Sie eine E-Mail an eine Mailbox-Simulator-Adresse senden, müssen Sie sie über Amazon SES senden, indem Sie das AWS CLI AWS SDK, die Amazon SES-Konsole, die Amazon SES SMTP-Schnittstelle oder die Amazon SES API verwenden. Der Postfachsimulator reagiert nicht auf E-Mails, die von externen Quellen empfangen werden.

Simuliertes Szenario	E-Mail-Adresse
Erfolgreiche Zustellung – Der E-Mail-An bieter des Empfängers akzeptiert Ihre E-Mail. Wenn Sie Lieferbenachrichtigungen wie unter Einrichten von Ereignisbenachrichtigungen für	success@simulator.amazonses.com

Simuliertes Szenario	E-Mail-Adresse
Amazon SES beschrieben einrichten, sendet Amazon SES Ihnen eine Lieferbenachrichtigung über Amazon Simple Notification Service (Amazon SNS).	
Unzustellbarkeit – Der E-Mail-Anbieter des Empfängers lehnt Ihre E-Mail mit dem SMTP-Antwortcode 550 5.1.1 („Unbekannter Benutzer“) ab. Amazon SES generiert eine Benachrichtigung über die Unzustellbarkeit und sendet sie Ihnen je nach Einrichtung Ihres Kontos per E-Mail oder als Benachrichtigung an ein Amazon-SNS-Thema. Die E-Mail-Adresse des Postfachsimulators wird nicht auf die Amazon-SES-Unterdrückungsliste gesetzt, wie es sonst bei einer permanenten Unzustellbarkeit der Fall ist. Die vom Postfachsimulator übermittelte Unzustellbarkeitsnachricht entspricht RFC 3464. Weitere Informationen zu Rückmeldungen im Falle von Unzustellbarkeit finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.	bounce@simulator.amazonses.com
Automatische Antworten – Der E-Mail-Anbieter des Empfängers akzeptiert Ihre E-Mail und sendet sie an dessen Posteingang. Der E-Mail-Anbieter sendet eine automatische Antwort, wie z. B. eine "außer Haus"-Abwesenheitsnachricht (out of the office, OOTO), an die Adresse im Return-Path-Header der E-Mail oder die Envelope-Absender („MAIL FROM“)-Adresse, wenn der Return-Path-Header nicht vorhanden ist. Die vom Postfachsimulator übermittelte automatische Nachricht entspricht RFC 3834.	ooto@simulator.amazonses.com

Simuliertes Szenario	E-Mail-Adresse
Beschwerde – Der E-Mail-Anbieter des Empfängers akzeptiert Ihre E-Mail und sendet sie an dessen Posteingang. Der Empfänger entscheidet, dass Ihre Nachricht unerwünscht ist und klickt in seinem E-Mail-Client auf „Als Spam markieren“. Amazon SES leitet dann die Beschwerdebenachrichtigung per E-Mail oder durch Benachrichtigung eines Amazon-SNS-Themas an Sie weiter, je nachdem, wie Sie Ihr Konto eingerichtet haben. Die vom Postfachs imulator übermittelte Beschwerdenachricht entspricht RFC 5965. Weitere Informationen zu Rückmeldungen im Falle von Beschwerd en finden Sie unter Einrichten von Ereignisb enachrichtigungen für Amazon SES.	complaint@simulator.amazonses.com
Empfängeradresse auf Unterdrückungslist e – Amazon SES generiert eine permanent e Unzustellbarkeit, als ob die Adresse des Empfängers auf der globalen Unterdrüc kungsliste steht.	suppressionlist@simulator.amazonses.com

Testen von Reject-Ereignissen

Jede von Ihnen über Amazon SES gesendete Nachricht wird auf Viren geprüft. Wenn Sie eine Nachricht senden, die einen Virus enthält, akzeptiert Amazon SES die Nachricht, erkennt den Virus und lehnt die gesamte Nachricht ab. Wenn Amazon SES die Nachricht ablehnt, hält es die Verarbeitung der Nachricht an und versucht nicht, sie dem E-Mail-Server des Empfängers zuzustellen. Anschließend wird ein Reject-Ereignis generiert.

Der Amazon-SES-Postfachsimulator enthält keine Adresse für das Testen von Reject-Ereignissen. Sie können Reject-Ereignisse jedoch mit einer EICAR-Testdatei (European Institute for Computer Antivirus Research) testen. Diese Datei ist eine sichere, branchenübliche Methode zum Testen von Antivirus-Software. Zum Erstellen einer EICAR-Testdatei fügen Sie den folgenden Text in eine Datei ein:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Speichern Sie die Datei unter `sample.txt`, fügen Sie ihr eine E-Mail-Adresse an und senden Sie die E-Mail an eine verifizierte Adresse. Sofern keine anderen Probleme mit der E-Mail vorliegen, akzeptiert Amazon SES die Nachricht, lehnt sie jedoch anschließend wie bei einer Datei mit einem tatsächlichen Virus ab.

> **Note**
>
> Abgelehnte E-Mails – einschließlich derjenigen, die Sie mit dem oben beschriebenen Verfahren senden – werden Ihrer täglichen Sendequote angerechnet. Jede Nachricht, die Sie senden, einschließlich derjenigen, die abgelehnt wurden, wird Ihnen in Rechnung gestellt.

Weitere Informationen zu EICAR-Testdateien finden Sie auf der EICAR-Testdateiseite auf Wikipedia.

Verwenden von Amazon SES-Konfigurationssätzen im

Konfigurationssätze sind Gruppen von Regeln, die Sie auf Ihre verifizierten Identitäten anwenden können. In Amazon SES bezeichnet Identität eine E-Mail-Adresse oder eine Domäne, die Sie zum Versenden von E-Mails verwenden. Wenn Sie einen Konfigurationssatz auf eine E-Mail anwenden, werden alle Regeln dieses Konfigurationssatzes auf die E-Mail angewendet.

Mit Hilfe von Konfigurationssätzen können Sie die folgenden Arten von Regeln auf den Versand von E-Mails anwenden und einen, beide oder keinen dieser Typen enthalten:

- Ziele für Ereignisse — Ermöglicht es Ihnen, für jede E-Mail, die Sie versenden, Statistiken zum E-Mail-Versand zu veröffentlichen, einschließlich der Anzahl der Sendungen, Zustellungen, Öffnungen, Klicks, Zurückweisungen und Beschwerden an andere AWS Produkte. Sie können beispielsweise Ihre E-Mail-Metriken an ein Amazon Data Firehose-Ziel senden und sie dann mit Amazon Managed Service for Apache Flink analysieren. Alternativ können Sie Unzustellbarkeits- und Beschwerdeinformationen an Amazon SNS senden und erhalten sofort Benachrichtigungen, wenn diese Ereignisse eintreten.
- IP-Pool-Verwaltung – Wenn Sie dedizierte IP-Adressen für die Verwendung mit Amazon SES leasen, können Sie Gruppen dieser Adressen erstellen, die als dedizierte IP-Pools bezeichnet werden, die zum Senden bestimmter E-Mail-Typen verwendet werden. Beispielsweise können Sie diese dedizierten IP-Pools Konfigurationssätze zuordnen und einen weiteren für den Versand von Marketingkommunikation und einen weiteren für den Versand von Transaktions-E-Mails verwenden. Ihre Absender-Reputation für transaktionale E-Mails wird dann von der für Ihre Marketing-E-Mails getrennt.

Um einen Konfigurationssatz mit einer überprüften Identität zuzuordnen, können Sie wie folgt vorgehen:

- Fügen Sie einen Verweis auf den Konfigurationssatz in den Kopfzeilen der E-Mail ein. Weitere Informationen zum Festlegen von Konfigurationssätzen in Ihren E-Mails finden Sie unter Festlegen eines Konfigurationssatzes für das Senden von E-Mail.
- Geben Sie einen vorhandenen Konfigurationssatz an, der als Standardkonfigurationssatz der Identität verwendet werden soll, entweder zum Zeitpunkt der Identitätserstellung oder später beim Bearbeiten einer verifizierten Identität. Siehe Grundlegendes zu den Standardkonfigurationssätzen.

Inhalt

- Verwalten der SES Konfigurationssätze
- Verwalten der Amazon-SES-Konfigurationssätze
- Festlegen eines Konfigurationssatzes für das Senden von E-Mail
- Reputationsmetriken anzeigen und exportieren

Verwalten der SES Konfigurationssätze

Sie können die SES Konsole, die`CreateConfigurationSet`-Aktion in der Amazon SES API v2 oder die`aws sesv2 create-configuration-set`Klicken Sie auf der Amazon SES CLI v2, um einen neuen Konfigurationssatz zu erstellen. In diesem Abschnitt wird erläutert, wie Sie Konfigurationssätze mit der SES Konsole und der Amazon SES CLI v2 erstellen.

So erstellen Sie einen Konfigurationssatz (Konsole)

So erstellen Sie einen Konfigurationssatz mithilfe der SES Konsole:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Klicken Sie im Navigationsbereich unter Configuration (Konfiguration), wählen Sie Configuration Sets (Konfigurationssätze) aus.
3. Wählen Sie Create route (Route erstellen) aus.
4. Allgemeine Informationen — Dieser Abschnitt enthält Optionen zur Anpassung Ihres Konfigurationssatzes:

    - Name des Konfigurationssatzes — Der Name für Ihren Konfigurationssatz. Der Name kann bis zu 64 alphanumerische Zeichen enthalten, einschließlich Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_).
    - IP-Pool senden — Wenn Sie E-Mails mit diesem Konfigurationssatz senden, werden Nachrichten von den dedizierten IP-Adressen im zugewiesenen Pool gesendet. Wählen Sie ein AMI aus der Liste aus.

    > **Note**
    >
    > Die Standardeinstellung (ses-default-dedicated-pool) enthält dedizierte IP-Adressen, die keinem anderen Pool zugewiesen wurden. Weitere Informationen zu IP-Pools finden Sie unter IP-Pols zuweisen.

- Optionen zur Nachverfolgung
  - Benutzerdefinierte Weiterleitungsdomäne verwenden — Aktivieren Sie das Kontrollkästchen, um eine benutzerdefinierte Weiterleitungsdomäne für die Nachverfolgung von Öffnungs- und Klickinformationen für E-Mails zu verwenden, die mit diesem Konfigurationssatz gesendet wurden.
  - Benutzerdefinierte Weiterleitungsdomain — Wählen Sie eine verifizierte Domain aus der Liste Wählen Sie eine verifizierte Domain als Ihre benutzerdefinierte Weiterleitungsdomain aus. Sie können auch eine Subdomain in das Feld Subdomain eingeben eingeben.

> **Note**
>
> Benutzerdefinierte Umleitungsdomänen können wie folgt angegeben werden:
>
> - Sie müssen zunächst eine benutzerdefinierte Weiterleitungsdomain in der E-Mail, die AWS-Region Sie senden und verfolgen möchten, erstellen und verifizieren sowie ein Content Delivery Network (CDN) einrichten. Dies wird unter erklärt. Konfigurieren von benutzerdefinierten Domänen zur Verarbeitung der Öffnungs- und Klicknachverfolgung
> - Um anschließend Ihre benutzerdefinierte Weiterleitungsdomäne für das Öffnen und Klicken zu verwenden, müssen Sie sie angeben, während Sie Ihren Konfigurationssatz hier in diesem Schritt erstellen oder bearbeiten.
> - Nachdem Sie Ihre benutzerdefinierte Umleitungsdomäne angegeben haben, wird View DNS Records schließlich im Container „Allgemeine Details“ des Konfigurationssatzes angezeigt. Wenn Sie ihn erweitern, sehen Sie den CNAME-Eintrag, der die Tracking-Domain enthält, die in Ihrem AWS-Region verwendet wird. Wenn Ihre benutzerdefinierte Subdomain beispielsweise marketing.example.com heißt und sie in der erstellt wurde AWS-Region **`us-east-1`**, würde die Erweiterung der View DNS-Einträge einen CNAME-Eintrag mit den folgenden Werten anzeigen: Name = marketing.example.com und Value = r.us-east-1.awstrack.me.
>
>   Sie können diese Informationen einfach als Bestätigung dafür verwenden, dass Sie bei der Einrichtung Ihres CDN die richtige Tracking-Domain aus der Tabelle ausgewählt haben, wie unter beschriebenKonfigurieren von benutzerdefinierten Domänen zur Verarbeitung der Öffnungs- und Klicknachverfolgung, oder Sie

können dies zuerst tun und die CNAME-Datensatzwerte von hier aus verwenden, um sie in Ihrem CDN-Setup zu verwenden.

- HTTPS-Richtlinie — Wählen Sie eine HTTPS-Richtlinienoption für das Protokoll des Öffnens und klicken Sie auf die Tracking-Links für Ihre benutzerdefinierte Weiterleitungsdomain:
  - Optional — (Standardverhalten) Offene Tracking-Links werden mit HTTP umschlossen. Links zur Klickverfolgung werden unter Verwendung des Originalprotokolls des Links umschlossen.
  - Erforderlich — Links zum Öffnen und Klicken werden beide mit HTTPS verpackt.
  - Erforderlich für Öffnungen — Offene Tracking-Links werden mit HTTPS umschlossen. Links zur Klickverfolgung werden unter Verwendung des Originalprotokolls des Links verpackt.
- Erweiterte Versandoptionen — Wählen Sie den Pfeil auf der linken Seite, um den Abschnitt mit den erweiterten Versandoptionen zu erweitern.
  - Transport Layer Security (TLS) — Wenn SES eine sichere Verbindung mit dem empfangenden Mailserver herstellen und E-Mails über das TLS-Protokoll versenden muss, aktivieren Sie das Kontrollkästchen Erforderlich.

> **Note**
>
> SES unterstützt TLS 1.2 und empfiehlt TLS 1.3. Weitere Informationen hierzu finden Sie unter Infrastruktursicherheit in SES.

  - Maximale Zustellungsdauer — Um ein Zeitlimit festzulegen, innerhalb dessen SES versuchen soll, E-Mails über diesen Konfigurationssatz zuzustellen, geben Sie einen Wert in Sekunden zwischen 300 und bis zu 50.400 ein.

> **Note**
>
> Die Festlegung eines benutzerdefinierten maximalen Zustelllimits (kürzer als der SES-Standard von 14 Stunden) kann in zeitkritischen E-Mails (z. B. solchen, die ein enthalten one-time-password), Transaktions-E-Mails und E-Mails, bei denen Sie sicherstellen möchten, dass sie außerhalb der Geschäftszeiten nicht zugestellt werden, nützlich sein.

> **Tip**
>
> - Um Minuten in Sekunden zu berechnen, multiplizieren Sie mit 60, z. B. 7 Minuten * 60 = 420 Sekunden.
> - Um Stunden in Sekunden zu berechnen, multiplizieren Sie mit 3600, z. B. 2 Stunden * 3600 = 7200 Sekunden.

5. Reputationsoptionen — In diesem Abschnitt können Sie Reputationsmetriken einrichten:

   - Reputationsmetriken — Wird verwendet, um Messwerte CloudWatch für E-Mails, die mit diesem Konfigurationssatz gesendet wurden, nachzuverfolgen, ob E-Mails zurückgesendet wurden. (Es fallen zusätzliche Gebühren an, siehe Preis pro Metrik für CloudWatch.)
     - Aktiviert — Wählen Sie dieses Kontrollkästchen, um Reputationsmetriken für den Konfigurationssatz zu aktivieren.

6. Optionen für die Unterdrückungsliste — Dieser Abschnitt enthält einen Entscheidungssatz zur Definition einer benutzerdefinierten Unterdrückung, beginnend mit der Option, diesen Konfigurationssatz zu verwenden, um Ihre Unterdrückung auf Kontoebene außer Kraft zu setzen. Die Logik-Map für die Unterdrückung auf Satzebene hilft Ihnen, die Auswirkungen der Überschreibungskombinationen zu verstehen. Diese mehrschichtige Auswahl an Überschreibungen kann kombiniert werden, um drei verschiedene Unterdrückungsebenen zu implementieren:

   a. Verwenden Sie Unterdrückung auf Kontoebene: Überschreiben Sie Ihre Unterdrückung auf Kontoebene nicht und implementieren Sie keine Unterdrückung auf Konfigurationssatzebene. Grundsätzlich verwendet jede E-Mail, die mit diesem Konfigurationssatz gesendet wird, nur Ihre Unterdrückung auf Kontoebene. So gehen Sie vor:

      - Deaktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

   b. Verwenden Sie keine Unterdrückung: Überschreiben Sie die Unterdrückung auf Kontoebene, ohne die Unterdrückung auf Konfigurationssatzebene zu aktivieren. Dies bedeutet, dass alle mit diesem Konfigurationssatz gesendeten E-Mails keine Unterdrückung

auf Kontoebene verwenden – mit anderen Worten, jede Unterdrückung wird aufgehoben. So gehen Sie vor:

i. Aktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

ii. Deaktivieren Sie in der Suppression list (Unterdrückungsliste) das Kontrollkästchen Enabled (Aktiviert).

c. Verwenden Sie die Unterdrückung auf Satzebene auf Konfiguration: Überschreiben Sie Ihre Unterdrückung auf Kontoebene mit benutzerdefinierten Einstellungen für Unterdrückungslisten, die in diesem Konfigurationssatz definiert sind. Dies bedeutet, dass jede E-Mail, die mit diesem Konfigurationssatz gesendet wird, nur ihre eigenen Unterdrückungseinstellungen verwendet und alle Unterdrückungseinstellungen auf Kontoebene ignoriert. So gehen Sie vor:

i. Aktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

ii. Wählen Sie in der Suppression list (Unterdrückungsliste) Enabled (Aktiviert) aus.

iii. Wählen Sie in Specify the reason(s)... (Geben Sie den Grund(e) an ...) einen der Unterdrückungsgründe für diese zu verwendende Konfiguration aus.

7. Virtual Deliverability Manager-Optionen — Dieser Abschnitt ist nur verfügbar, wenn Sie die Funktionen von Virtual Deliverability Manager aktiviert haben. Hier können Sie benutzerdefinierte Einstellungen dafür definieren, wie dieser Konfigurationssatz das Engagement-Tracking und die optimierte gemeinsame Bereitstellung verwendet, indem Sie die Definition in Ihren Virtual Deliverability Manager-Einstellungen auf Kontoebene außer Kraft setzen:

a. Gehen Sie wie folgt vor, um sowohl das Engagement-Tracking als auch die optimierte gemeinsame Zustellung für diesen Konfigurationssatz zu deaktivieren:

i. Markieren Sie das Feld Override account level settings (Einstellungen auf Kontoebene überschreiben).

ii. Vergewissern Sie sich, dass Enabled (Aktiviert) sowohl für die Interaktionsnachverfolgung als auch für die optimierte gemeinsame Zustellung deaktiviert ist, und wählen Sie dann Save changes (Änderungen speichern) aus.

b. Gehen Sie wie folgt vor, um sowohl die die Interaktionsnachverfolgung als auch die optimierte gemeinsame Zustellung zu aktivieren oder zu deaktivieren:

   i. Markieren Sie das Feld Override account level settings (Einstellungen auf Kontoebene überschreiben).

   ii. Aktivieren oder deaktivieren Sie Enabled (Aktiviert) sowohl für die Engagement tracking (Interaktionsnachverfolgung), die Optimized shared delivery (optimierte gemeinsame Zustellung) oder beides, und wählen Sie dann Save changes (Änderungen speichern) aus.

c. Gehen Sie wie folgt vor, um zu den Einstellungen Ihres Kontos des virtuellen Zustellbarkeitsmanagers für die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung für diesen Konfigurationssatz zurückzukehren:

   • Löschen Sie das Häkchen im Feld Override account level settings (Einstellungen auf Kontoebene überschreiben) und wählen Sie dann Save changes (Änderungen speichern).

8. Archivierungsoptionen — Dieser Abschnitt bietet die Option zum Archivieren von E-Mails, die über diesen Konfigurationssatz gesendet wurden:

   a. Markieren Sie das Kontrollkästchen Enabled (Aktiviert).

   b. Klicken Sie in das Feld Archiv und wählen Sie ein Archiv aus der Liste, gefolgt von Änderungen speichern, oder wählen Sie Archiv erstellen und fahren Sie mit den verbleibenden Schritten fort.

   c. Geben Sie im Feld Archivname einen eindeutigen Namen ein.

   d. (Optional) Wählen Sie im Feld Aufbewahrungszeitraum einen Aufbewahrungszeitraum aus, um den standardmäßigen Aufbewahrungszeitraum von 180 Tagen zu überschreiben.

   e. (Optional) Sie können Ihr Archiv verschlüsseln, indem Sie entweder Ihren eigenen AWS KMS Schlüssel in das ARN-Feld KMS-Schlüssel eingeben oder indem Sie AWS KMS-Schlüssel erstellen auswählen.

   f. Wählen Sie Archiv erstellen.

9. Tags — In diesem Abschnitt können Sie optional ein oder mehrere Tags zu Ihrem Konfigurationssatz hinzufügen:

   a. Wählen Sie Add new tag (Neues Tag hinzufügen) aus.

   b. Geben Sie das Tag Key (Schlüssel) ein.

c. Geben Sie das Tag Value (Wert) ein (optional).

Zum Entfernen eines eingegebenen Tags wählen Sie Remove (Entfernen) für dieses Tag. Sie können maximal 50 Tags hinzufügen.

10. Wählen Sie Create set (Satz erstellen) zum Erstellen Ihres Konfigurationssatzes.

Nachdem Sie nun Ihren Konfigurationssatz erstellt haben, können Sie Ereignisziele für den Konfigurationssatz definieren. Dies ermöglicht die Ereignisveröffentlichung, die bei den Ereignistypen ausgelöst wird, die Sie für das Ereignisziel angeben. Ein Konfigurationssatz kann über mehrere Ereignisziele mit mehreren Ereignistypen verfügen. Siehe Erstellen von Amazon-SES-Ereigniszielen.

Konfigurationssatz erstellen (AWS CLI)

Sie können einen Konfigurationssatz mit einer JSON-Datei als Eingabe für die`aws sesv2 create-configuration-set`-Befehl in der AWS CLI aus.

1. Erstellen einer CLI-Eingabe-JSON-Datei

   Verwenden Sie Ihr bevorzugtes Dateibearbeitungswerkzeug, um eine JSON-Datei mit den folgenden Schlüsseln und Werten zu erstellen, die für Ihre Umgebung gültig sind, oder verwenden Sie den `aws sesv2 create-configuration-set`-Befehl der SES-API-v2 mit der `--generate-cli-skeleton`-Option ohne einen Wert anzugeben, um eine Beispiel-JSON-Struktur in die Standardausgabe zu drucken.

   In diesem Beispiel wird eine Datei mit dem Namen`create-configuration-set.json`:

```
{
    "ConfigurationSetName": "sample-configuration-set",
    "TrackingOptions": {
        "CustomRedirectDomain": "some.domain.com",
        "HttpsPolicy": "REQUIRE"
    },
    "DeliveryOptions": {
        "TlsPolicy": "REQUIRE",
        "SendingPoolName": "sending pool",
        "MaxDeliverySeconds": 300
    },
    "ReputationOptions": {
        "ReputationMetricsEnabled": true,
```

```
        "LastFreshStart": timestamp
    },
    "SendingOptions": {
        "SendingEnabled": true
    },
    "Tags": [
        {
            "Key": "tag key",
            "Value": "tag value"
        }
    ],
    "SuppressionOptions": {
        "SuppressedReasons": ["BOUNCE","COMPLAINT"]
    },
    "ArchivingOptions": {
        "ArchiveArn": "arn:aws:ses:us-east-1:123456789012:mailmanager-
archive/MyArchiveID"
    }
}
```

> **Note**
>
> - Sie müssen die`file://`-Notation am Anfang des JSON-Dateipfades.
> - Der Pfad für die JSON-Datei sollte der entsprechenden Konvention für das Basisbetriebssystem folgen, auf dem Sie den Befehl ausführen. Windows verwendet beispielsweise den umgekehrten Schrägstrich (\), um auf den Verzeichnispfad zu verweisen, und Linux verwendet den Schrägstrich (/).

2. Führen Sie den folgenden Befehl aus, indem Sie die Datei verwenden, die Sie als Eingabe erstellt haben.

```
aws sesv2 create-configuration-set --cli-input-json file://create-configuration-
set.json
```

> **Note**
>
> Die AWS CLI Referenz zu diesem Befehl finden Sie unter create-configuration-set.

Verwalten der Amazon-SES-Konfigurationssätze

Nachdem Sie einen Konfigurationssatz erstellt haben, können Sie ihn mit den Optionen zum Anzeigen, Bearbeiten und Löschen mit der SES-Konsole, der Amazon-SES-API v2 und der Amazon-SES-CLI v2 verwalten. Konfigurationssätze können auch einer verifizierten Identität als Standardkonfigurationssatz zugewiesen werden, der jedes Mal angewendet wird, wenn E-Mails von der Identität gesendet werden.

Themen in diesem Abschnitt:

- Konfigurationssatz anzeigen, bearbeiten und löschen (Konsole)
- Konfigurationssätze auflisten (AWS CLI)
- Details zum Konfigurationssatz abrufen (AWS CLI)
- Löschen eines Konfigurationssatzes (AWS CLI)
- Beenden Sie das Senden von E-Mails aus einem Konfigurationssatz (AWS CLI)
- Grundlegendes zu den Standardkonfigurationssätzen
- Erstellen von Amazon-SES-Ereigniszielen
- Zuweisen von IP-Pools in Amazon SES
- Konfigurieren von benutzerdefinierten Domänen zur Verarbeitung der Öffnungs- und Klicknachverfolgung

Konfigurationssatz anzeigen, bearbeiten und löschen (Konsole)

Greifen Sie auf die Detailseite eines vorhandenen Konfigurationssatzes zu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Configuration sets (Konfigurationssätze) aus.
3. Wählen Sie einen Namen aus der Liste der Konfigurationssätze aus, um die zugehörige Detailseite auf der Registerkarte „Übersicht“ zu öffnen, auf der Sie die ausgewählten Optionen anzeigen, bearbeiten oder deaktivieren können. Dasselbe können Sie für die Zieloptionen für Ereignisse tun, indem Sie die entsprechende Registerkarte auswählen. Weitere Informationen zu den einzelnen Optionen und ihren Feldern finden Sie im entsprechenden Abschnitt unterSo erstellen Sie einen Konfigurationssatz (Konsole).

4. Oben auf der Detailseite der einzelnen Konfigurationssätze, die entweder über die Registerkarte Übersicht oder das Ziel der Ereignisse sichtbar ist, befinden sich die folgenden Optionen:

   - Löschen – diese Schaltfläche löscht Ihren Konfigurationssatz.
   - Deaktivieren Sie das Senden – diese Schaltfläche stoppt das Senden von E-Mails aus Ihrem Konfigurationssatz.

Konfigurationssätze auflisten (AWS CLI)

Sie können den list-configuration-sets Befehl in der verwenden AWS CLI , um eine Liste aller mit Ihrem Konto verknüpften Konfigurationssätze in der aktuellen Region wie folgt zu generieren:

```
aws sesv2 list-configuration-sets
```

Details zum Konfigurationssatz abrufen (AWS CLI)

Sie können den get-configuration-set Befehl in der verwenden AWS CLI , um Details zu einem bestimmten Konfigurationssatz wie folgt abzurufen:

```
aws sesv2 get-configuration-set --configuration-set-name name
```

Löschen eines Konfigurationssatzes (AWS CLI)

Sie können den delete-configuration-set Befehl in der verwenden AWS CLI , um einen bestimmten Konfigurationssatz wie folgt zu löschen:

```
aws sesv2 delete-configuration-set --configuration-set-name name
```

Beenden Sie das Senden von E-Mails aus einem Konfigurationssatz (AWS CLI)

Sie können den put-configuration-set-sending-options Befehl in verwenden AWS CLI , um das Senden von E-Mails aus einem bestimmten Konfigurationssatz wie folgt zu beenden:

```
aws sesv2 put-configuration-set-sending-options --configuration-set-name name --no-
sending-enabled
```

Wenn Sie erneut mit dem Senden beginnen, führen Sie denselben Befehl mit der`--sending-enabled`Verwenden Sie stattdessen folgendes:

```
aws sesv2 put-configuration-set-sending-options --configuration-set-name name --sending-enabled
```

Grundlegendes zu den Standardkonfigurationssätzen

Das Konzept der Zuweisung einer Konfiguration, die als Standard festgelegt ist, die von einer verifizierten Identität verwendet wird, wird in diesem Abschnitt erläutert, um die Vorteile und den Anwendungsfall zu verstehen.

Die Regeln eines Standardkonfigurationssatzes werden automatisch auf alle Nachrichten angewendet, die Sie von der E-Mail-Identität senden, die diesem Konfigurationssatz zugeordnet ist. Sie können Standardkonfigurationssätze sowohl auf E-Mail-Adresse als auch auf Domänenidentitäten während der Erstellung der Identität oder danach als Bearbeitungsfunktion einer vorhandenen Identität anwenden.

Default configuration set considerations (Überlegungen zum Standardkonfigurationssatz)

- Der Konfigurationssatz muss zuerst erstellt werden, bevor er einer Identität zugeordnet wird.
- Standardkonfigurationssätze werden nur angewendet, wenn die Identität überprüft wird.
- Eine E-Mail-Identität kann jeweils nur einem Konfigurationssatz zugeordnet werden. Sie können jedoch denselben Konfigurationssatz auf mehrere Identitäten anwenden.
- Die Regeln eines Standardkonfigurationssatzes werden automatisch auf alle Nachrichten angewendet, die Sie von der E-Mail-Identität senden, die diesem Konfigurationssatz zugeordnet ist. Beispielsweise hat ein Standardkonfigurationssatz, der joe@example.com zugeordnet ist, Vorrang vor dem Konfigurationssatz für die Domäne example.com.
- Ein auf Domänenebene festgelegter Standardkonfigurationssatz gilt für alle E-Mail-Adressen dieser Domäne (es sei denn, Sie überprüfen bestimmte Adressen für die Domäne).
- Wenn Sie einen Konfigurationssatz löschen, der als Standardkonfigurationssatz für eine Identität festgelegt ist, und dann versuchen, E-Mails über diese Identität zu senden, schlägt Ihr Aufruf von Amazon SES mit einem „Bad Request“-Fehler fehl.
- Ein Standardkonfigurationssatz kann keiner verifizierten Identität zugewiesen werden, die von einem delegierten Sender verwendet wird.

- So geben Sie einen vorhandenen Konfigurationssatz an, der verwendet werden soll, da der Standardkonfigurationssatz der Identität tatsächlich eine Funktion verifizierter Identitäten ist, daher werden Anweisungen in den Identitätsworkflows entsprechend angegeben:
  - Geben Sie während der Identitätserstellung einen Standardkonfigurationssatz an – befolgen Sie die Anweisungen im optionalen Schritt 6 für den Standardkonfigurationssatz für die Domänenidentität oder den Standardkonfigurationssatz für die E-Mail-Identität im Kapitel Erstellen und verifizieren von Identitäten in Amazon SES.
  - Geben Sie einen Standardkonfigurationssatz für eine vorhandene Identität an – führen Sie die Schritte in Bearbeiten Sie eine Identität mit der Konsole zusammen mit diesen Details für Schritt 5 aus:
    a. Wählen Sie die Registerkarte Configuration set (Konfigurationssatz) aus.
    b. Wählen Sie Edit (Bearbeiten) im Container Default configuration set (Standardkonfigurationssatz) aus.
    c. Wählen Sie das Listenfeld aus und wählen Sie einen vorhandenen Konfigurationssatz aus, der als Standard verwendet werden soll.
    d. Fahren Sie mit den restlichen Schritten unter Bearbeiten Sie eine Identität mit der Konsole fort.

> **Note**
>
> Wenn für den Konfigurationssatz, den Sie als Standard zuweisen, Reputationsmetriken aktiviert sind, fallen zusätzliche Gebühren für alle E-Mails an, die mit dem Standardkonfigurationssatz gesendet werden. Weitere Informationen finden Sie unter Preis pro Metrik für CloudWatch.

Erstellen von Amazon-SES-Ereigniszielen

Mithilfe von Ereigniszielen können Sie die folgenden Aktionen zur Nachverfolgung ausgehender E-Mails an andere AWS Dienste zur Überwachung veröffentlichen:

- Sends (Sendevorgänge)
- Rendering failures (Rendern von Fehlern)
- Rejects (Ablehnen)
- Deliveries (Zustellungen)

- Hard bounces (Permanente Unzustellbarkeiten)
- Complaints (Beschwerden)
- Delivery delays (Verzögerungen von Lieferungen)
- Subscriptions (Abonnements)
- Opens (Öffnungsvorgänge)
- Clicks (Klickvorgänge)

Weitere Informationen zum Einrichten der Ereignisveröffentlichung finden Sie unter the section called “Überwachen des E-Mail-Versands mithilfe der Ereignisveröffentlichung”.

Erstellen eines Ereignisziels

Nachdem Sie einen Konfigurationssatz erstellt haben, können Sie Ereignisziele für den Konfigurationssatz erstellen. Dies ermöglicht die Ereignisveröffentlichung, die bei den Ereignistypen ausgelöst wird, die Sie für das Ereignisziel angeben. Ein Konfigurationssatz kann über mehrere Ereignisziele mit mehreren Ereignistypen verfügen.

Wenn Sie noch keinen Konfigurationssatz erstellt haben, informieren Sie sich unter the section called “Erstellen Sie einen Konfigurationssatz.”.

Die folgenden Schritte zeigen, wie Sie ein Ereignisziel erstellen oder einem Konfigurationssatz hinzufügen.

So können Sie ein Ereignisziel mithilfe der SES-Konsole erstellen oder hinzufügen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Configuration sets (Konfigurationssätze) aus.
3. Wählen Sie in der Spalte Name den Namen eines Konfigurationssatzes aus, um die Details aufzurufen.
4. Wählen Sie die Registerkarte Event destinations (Ereignisziele) aus.
5. Wählen Sie Add destination (Ziel hinzufügen).

6. Wählen Sie alle Einträge unter Event types aus.

   E-Mail-Versandereignisse sind Metriken, die sich auf Ihre Sendeaktivitäten beziehen, die Sie mit Amazon SES messen können. In diesem Schritt wählen Sie aus, welche Arten von E-Mail-Nachrichten gesendet werden sollen, die Amazon SES an Ihrem Ereignisziel veröffentlichen soll.

   Weitere Informationen zu den Richtlinientypen finden Sie unter Überwachen Ihrer Amazon SES-Sendeaktivität.

   a. Klicken Sie auf Event types (Ereignistypen) veröffentlichen Sie das

      - Versand und Zustellung – um die zu veröffentlichenden Ereignistypen auszuwählen, aktivieren Sie die entsprechenden Kontrollkästchen oder wählen SieAlle auswählen, um alle Ereignistypen zu veröffentlichen.

        Event types (Ereignistypen)

        - Sends (Sendevorgänge) – die Sendeanfrage war erfolgreich und Amazon SES versucht, dem E-Mail-Server des Empfängers die Nachricht zuzustellen.
        - Rendering failures (Rendern von Fehlern) – Die E-Mail wurde aufgrund eines Rendering-Problems mit der Vorlage nicht gesendet. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail-Vorlage mithilfe der `SendTemplatedEmail`- oder `SendBulkTemplatedEmail`-API-Operationen senden.
        - Rejects (Ablehnungen) – Amazon SES hat die E-Mail akzeptiert, aber festgestellt, dass sie einen Virus enthielt und nicht versucht hat, ihn an den Mail-Server des Empfängers zu übermitteln.
        - Deliveries (Zustellungen) – Amazon SES hat die E-Mail erfolgreich an den E-Mail-Server des Empfängers übermittelt.
        - Bounces (Unzustellbarkeiten) – Die E-Mail wurde vom E-Mail-Server des Empfängers dauerhaft abgelehnt. (Soft bounces (Temporäre Unzustellbarkeiten) werden nur dann aufgenommen, wenn Amazon SES über einen bestimmten Zeitraum vergeblich versucht hat, die E-Mail zuzustellen.)
        - Complaints (Beschwerden) – die E-Mail wurde erfolgreich an den E-Mail-Server des Empfängers gesendet, der Empfänger hat sie jedoch als Spam markiert.
        - Delivery Delays (Verzögerungen von Bereitstellungen) – Die E-Mail konnte nicht an den Empfänger gesendet werden, da ein vorübergehendes Problem aufgetreten ist.

Verzögerungen bei der Zustellung können, z. B. auftreten, wenn der Posteingang des Empfängers voll ist oder der empfangende E-Mail-Server ein vorübergehendes Problem aufweist. (Dieser Ereignistyp wird von Amazon Pinpoint nicht unterstützt.)

- Subscriptions (Abonnements) – die E-Mail wurde erfolgreich zugestellt, aber der Empfänger hat die Abonnementeinstellungen aktualisiert, indem er auf`List-Unsubscribe`in der E-Mail-Kopfzeile oder im`Unsubscribe`-Link in der Fußzeile erstellt. (Dieser Ereignistyp wird von Amazon Pinpoint nicht unterstützt.)

- Open and click tracking (Nachverfolgung öffnen und anklicken) – um die Teilnehmerinteraktion zu messen, wählen Sie eines oder beide Kontrollkästchen aus, die Sie verfolgen möchten Opens (Öffnungsvorgänge) und Clicks (Klickvorgänge) aus.
  - Opens (Öffnungen) – Der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
  - Clicks (Klicks) – Der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.

    > **Note**
    >
    > Die hier oder in einem anderen Konfigurationssatz definierte Ereignisveröffentlichung für Öffnungs- und Klickereignisse wirkt sich dies nicht auf die Optionen der Interaktionsnachverfolgung für das Dashboard des virtuellen Zustellbarkeitsmanagers aus. Diese werden entweder durch die Kontoeinstellungen des virtuellen Zustellbarkeitsmanagers oder durch Überschreibungen des Konfigurationssatzes definiert. Wenn Sie beispielsweise die Interaktionsnachverfolgung über den virtuellen Zustellbarkeitsmanager deaktiviert haben, wird die Ereignisveröffentlichung für Öffnungs- und Klickereignisse, die Sie hier in den SES-Ereigniszielen eingerichtet haben, nicht deaktiviert.

  - Configuration set redirect domain (Konfigurationssatz-Umleitungsdomäne) – Dieses Feld wird angezeigt und wird mit dem Namen der benutzerdefinierten Umleitungsdomäne vorausgefüllt, wenn Sie beim Erstellen des Konfigurationssatzes eine zugewiesen haben.

    > **Note**
    >
    > Sie können die Custom redirect domain (Benutzerdefinierte Umleitungsdomain) im Konfigurationssatz für die Nachverfolgung für Öffnen und Klicken unter dieser Domain aktualisieren – siehe Nachverfolgungsoptionen in Schritt 4

von Erstellen Sie einen Konfigurationssatz.. Weitere Informationen zur Konfiguration von benutzerdefinierten Öffnungs- und Klickdomänen finden Sie unterKonfigurieren von benutzerdefinierten Domänen zur Verarbeitung der Öffnungs- und Klicknachverfolgungaus.

b. Wählen Sie Next (Weiter), um fortzufahren.

7. Ziel angeben

Ein Event-Ziel ist ein AWS Service, über den Ereignisse, die per E-Mail versendet werden, veröffentlicht werden können. Welches Ziel ausgewählt wird, hängt davon ab, wie detailliert die Daten sein sollen und auf welche Art und Weise Sie erfassen möchten.

a. destination: optional.

- Zieltyp — Wenn Sie das Optionsfeld neben dem AWS Dienst auswählen, für den Sie Ihre Ereignisse veröffentlichen möchten, wird ein Detailbereich mit den entsprechenden Feldern für den Dienst angezeigt. Wenn Sie die folgenden Links auswählen, erhalten Sie Anweisungen zum Detailbereich des Dienstes:
  - Amazon CloudWatch (Es fallen zusätzliche Gebühren an, siehe Preis pro Metrik für CloudWatch.)
  - Amazon Data Firehose
  - Amazon EventBridge
  - Amazon Pinpoint (Unterstützt die Ereignistypen Delivery delays (Zustellungsverzögerungen) und Subscriptions (Abonnements) nicht.)
  - Amazon SNS

  Weitere Informationen zur Überwachung des E-Mail-Vorgangs mithilfe des Ereignisveröffentlichungsmodells finden Sie unterÜberwachen des E-Mail-Versands mithilfe der Amazon SES-Ereignisveröffentlichungaus.
- NameGeben Sie den Namen des Ziels für diesen Konfigurationssatz ein. Der Name darf nur Buchstaben, Zahlen und Bindestriche enthalten.
- Event publishing (Ereignisveröffentlichung) – um die Ereignisveröffentlichung für dieses Ziel zu aktivieren, wählen Sie das KontrollkästchenEnabled.

b. Wählen Sie Next (Weiter), um fortzufahren.

8. Prüfen

   Wenn Sie mit der Richtigkeit Ihrer Einträge zufrieden sind, wählen Sie Add destination (Ziel hinzufügen) zum Hinzufügen Ihres Ereignisziels.

Sie können ein Ereignisziel auch über die Amazon-SES-Konsole, die Amazon-SES-API v2 oder die Amazon-SES-CLI v2 erstellen.

So erstellen Sie ein Ereignisziel mithilfe der SES-API:

- Informationen zum Erstellen eines Ereignisziels mithilfe der SES-API finden Sie unter `CreateConfigurationSetEventDestination`.

Bearbeiten, Aktivieren/Deaktivieren oder Löschen eines Ereignisziels

Gehen Sie folgendermaßen vor, um ein Ereignisziel mithilfe der SES-Konsole zu bearbeiten, zu deaktivieren/aktivieren oder zu löschen:

So bearbeiten, deaktivieren/aktivieren oder löschen Sie ein Ereignisziel mithilfe der SES-Konsole:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Configuration sets (Konfigurationssätze) aus.
3. Wählen Sie in der Spalte Name den Namen eines Konfigurationssatzes aus, um die Details aufzurufen.
4. Wählen Sie die Registerkarte Event destinations (Ereignisziele) des Konfigurationssatzes aus.
5. Wählen Sie den Namen des Ereignisziels unter der Spalte Name aus.
6. - Bearbeiten – Wählen Sie die Schaltfläche Edit (Bearbeiten) im entsprechenden Bereich für die Felder aus, die Sie bearbeiten möchten. Nehmen Sie Ihre Änderungen vor und klicken Sie auf Save changes (Änderungen speichern).
   - Deaktivieren oder aktivieren – Wählen Sie oben rechts die Schaltfläche mit der Bezeichnung Disable (Deaktivieren) bzw. Enable (Aktivieren) aus.
   - Löschen – Wählen Sie oben rechts die Schaltfläche Delete (Löschen) aus.

Sie können ein Ereignisziel auch über die Amazon-SES-Konsole, die Amazon-SES-API v2 oder die Amazon-SES-CLI v2 bearbeiten, deaktivieren/aktivieren oder löschen.

So bearbeiten, deaktivieren/aktivieren oder löschen Sie ein Ereignisziel mithilfe der SES-API:

1. Informationen zu disabling/enabling einem Veranstaltungsziel, das die SES-API verwendet, finden Sie unter `UpdateConfigurationSetEventDestination`.
2. Informationen zum Löschen eines Ereignisziels mithilfe der SES-API finden Sie unter `DeleteConfigurationSetEventDestination`.

Zuweisen von IP-Pools in Amazon SES

Mit IP-Pools können Sie Gruppen aus dedizierten IP-Adressen erstellen, mit denen bestimmte E-Mail-Typen gesendet werden. Sie können auch einen IP-Adresspool nutzen, der für alle Amazon-SES-Kunden verfügbar ist.

Sie können beim Zuweisen eines IP-Pools zu einem Konfigurationssatz folgende Optionen festlegen:

- Bestimmter dedizierter IP-Pool – Bei Auswahl eines vorhandenen dedizierten IP-Pools werden E-Mails, die diesen Konfigurationssatz verwenden, ausschließlich über die dedizierten IP-Adressen in diesem Pool gesendet. Anleitungen zum Erstellen:
  - Neue Standard-IP-Pools: siehe Erstellung von standardmäßigen dedizierten IP-Pools für dedizierte IPs (Standard).
  - Neue verwaltete IP-Pools: siehe Erstellen eines verwalteten IP-Pools zur Aktivierung eines dedizierten (verwalteten) IPs.
- ses-default-dedicated-pool— Dieser Pool enthält alle dedizierten IP-Adressen für Ihr Konto, die noch nicht zu einem IP-Pool gehören. Wenn Sie eine E-Mail mit einem Konfigurationssatz senden, der keinem Pool zugeordnet ist, oder wenn Sie eine E-Mail senden, ohne überhaupt einen Konfigurationssatz anzugeben, wird die E-Mail von einer der Adressen in diesem Standardpool gesendet. Dieser Pool wird automatisch von SES verwaltet und kann nicht bearbeitet werden.
- ses-shared-pool— Dieser Pool enthält eine große Anzahl von IP-Adressen, die von allen Amazon SES SES-Kunden gemeinsam genutzt werden. Diese Option kann sinnvoll sein, wenn Sie E-Mails senden müssen, die nicht Ihrem üblichen Sendeverhalten entsprechen.

Zuweisen eines IP-Pools zu einem Konfigurationssatz

Dieser Abschnitt verweist auf die Verfahren zum Zuweisen und Ändern von IP-Pools in einem Konfigurationssatz mit der Amazon SES Konsole.

- So weisen Sie einen IP-Pool einem Konfigurationssatz zu...
  - Beim Erstellen eines neuen Konfigurationssatzes – siehe Sendungs-IP-Pool Schritt 4 von Erstellen Sie einen Konfigurationssatz.
  - während Sie einen vorhandenen Konfigurationssatz ändern – wählen Sie die Schaltfläche Edit (Bearbeiten) im Bereich General details (Allgemeine Details) des ausgewählten Konfigurationssatzes und befolgen Sie die Anweisungen zum Sending IP pool (IP-Pool senden) in Schritt 4 von Erstellen Sie einen Konfigurationssatz.

Konfigurieren von benutzerdefinierten Domänen zur Verarbeitung der Öffnungs- und Klicknachverfolgung

Wenn Sie die Ereignisveröffentlichung verwenden, um Öffnungs- und Klickereignisse zu erfassen, nimmt Amazon SES kleinere Änderungen an den von Ihnen gesendeten E-Mails vor. Zum Erfassen von Öffnungsereignissen fügt SES in jeder über SES gesendeten E-Mail ein transparentes GIF-Bild mit einer Breite und Höhe von jeweils 1 Pixel ein, das einen eindeutigen Dateinamen für jede E-Mail enthält und auf einem von SES betriebenen Server gehostet wird. Wenn das Bild heruntergeladen wird, kann SES genau feststellen, welche Nachricht von wem geöffnet wurde.

Standardmäßig wird dieses Pixel am Ende der E-Mail eingefügt. Die Anwendungen einiger E-Mail-Anbieter beschneiden jedoch die Vorschau einer E-Mail, wenn sie eine bestimmte Größe überschreitet, und stellen möglicherweise einen Link zur Anzeige der restlichen Nachricht zur Verfügung. In diesem Szenario wird das SES-Pixelbild zur Nachverfolgung nicht geladen und verfälscht die Öffnungsraten, die Sie nachverfolgen möchten. Um dies zu umgehen, können Sie das Pixel optional an den Anfang der E-Mail oder an eine andere Stelle setzen, indem Sie den Platzhalter `{{ses:openTracker}}` in den E-Mail-Text einfügen. Sobald SES die Nachricht mit dem Platzhalter empfängt, wird sie durch ein Pixelbild zur Nachverfolgung von Öffnungen ersetzt.

> **Important**
>
> - Alle `{{ses:openTracker}}` Platzhalter, die mehr als einen Platzhalter enthalten, werden beim Versand durch SES entfernt.

- Fügen Sie nur einen `{{ses:openTracker}}` Platzhalter hinzu, wenn Sie ihn in einer E-Mail-Vorlage verwenden, da mehrere Platzhalter dazu führen, dass ein `400 BadRequestException` Fehlercode zurückgegeben wird.

Um Ereignisse mit Linkklicks zu erfassen, ersetzt SES die Links in Ihren E-Mails durch Links zu einem von SES betriebenen Server. Dadurch wird der Empfänger sofort an sein ausgewähltes Ziel weitergeleitet. Die Gesamtgröße der Header, einschließlich Cookies, der Anfragen an diesen Server darf 8192 Byte nicht überschreiten, andernfalls wird ein `400 BadRequestException` Fehlercode zurückgegeben.

Sie haben auch die Möglichkeit, Ihre eigenen Domains anstelle von Domains zu verwenden, die SES gehören und von SES betrieben werden, um Ihren Empfängern ein einheitlicheres Erlebnis zu bieten, d. h. alle SES-Indikatoren werden entfernt. Sie können mehrere benutzerdefinierte Domänen konfigurieren, um Öffnungs- und Klicknachverfolgungsereignisse zu verarbeiten. Diese benutzerdefinierten Domänen stehen im Zusammenhang mit Konfigurationssätzen. Wenn Sie eine E-Mail mit einem Konfigurationssatz senden und wenn dieser Konfigurationssatz für die Verwendung einer benutzerdefinierten Domäne konfiguriert ist, verwenden die Öffnungs- und Klicklinks in dieser E-Mail automatisch die benutzerdefinierte Domäne, die in diesem Konfigurationssatz angegeben ist.

Dieser Abschnitt enthält Verfahren zur Einrichtung einer Subdomain auf einem Server, den Sie besitzen, um Benutzer automatisch zu den von SES betriebenen Open- und Click-Tracking-Servern weiterzuleiten. Die Einrichtung dieser Domänen umfasst drei Schritte. Zuerst konfigurieren Sie die Subdomäne selbst. Dann legen Sie einen Konfigurationssatz zur Verwendung der benutzerdefinierten Domäne fest. Anschließend legen Sie das Ereignisziel zur Veröffentlichung von Öffnungs- und Klickereignissen fest. In diesem Abschnitt werden Verfahren für alle drei Schritte beschrieben.

Wenn Sie jedoch einfach die Öffnungs- oder Klicknachverfolgung aktivieren möchten, ohne eine benutzerdefinierte Domäne einzurichten, können Sie direkt mit der Definition von Ereigniszielen für Ihren Konfigurationssatz fortfahren. Dies ermöglicht die Ereignisveröffentlichung, die bei den angegebenen Ereignistypen ausgelöst wird, einschließlich Öffnungs- und Klickereignissen. Ein Konfigurationssatz kann über mehrere Ereignisziele mit mehreren Ereignistypen verfügen. Siehe Erstellen von Amazon-SES-Ereigniszielen.

Teil 1: Einrichten einer Domäne für die Verarbeitung der Umleitungen von Öffnungs- und Klicklinks

Die spezifische Vorgehensweise zum Einrichten einer Umleitungsdomäne hängt vom Ihrem Webhosting-Anbieter (und Ihrem Netzwerk zur Bereitstellung von Inhalten, wenn Sie einen HTTPS-Server verwenden) ab. Die Verfahren in den folgenden Abschnitten bieten allgemeine Richtlinien und nicht bestimmte Schritte.

Option 1: Konfigurieren einer HTTP-Domäne

Wenn Sie vorhaben, eine HTTP-Domäne für die Verarbeitung von Öffnungs- und Klicklinks zu verwenden (im Gegensatz zu einer HTTPS-Domäne), umfasst der Konfigurationsvorgang für die Subdomäne nur ein paar Schritte.

> **Note**
>
> Wenn Sie eine benutzerdefinierte Domäne einrichten die das HTTP-Protokoll verwendet, und eine E-Mail mit Links senden, die das HTTPS-Protokoll verwendet, sehen Ihre Kunden möglicherweise eine Warnmeldung, wenn sie auf die Links in Ihrer E-Mail klicken. Wenn Sie vorhaben, E-Mails mit Links zu senden, die das HTTPS-Protokoll verwenden, sollten Sie eine HTTPS-Domäne für die Verarbeitung von Klicknachverfolgungsereignissen verwenden.

So richten Sie eine HTTP-Subdomäne für die Verarbeitung von Öffnungs- und Klicklinks ein

1. Erstellen Sie eine Subdomäne zur Verwendung für Öffnungs- und Klicknachverfolgungs-Links. SES empfiehlt, dass diese Subdomain speziell für die Verarbeitung dieser Links vorgesehen ist und dass für jede von Ihnen gesendete E-Mail, die AWS-Region Sie verfolgen möchten, eine Subdomain erstellt wird.
2. Überprüfen Sie die Subdomain für die Verwendung mit SES. Weitere Informationen finden Sie unter Erstellen einer Domänenidentität.
3. Fügen Sie den DNS-Einstellungen Ihrer Subdomain einen neuen CNAME-Eintrag hinzu, der Anfragen an die SES-Tracking-Domain umleitet. Die Adresse, zu der Sie weiterleiten, muss mit Ihrer benutzerdefinierten Subdomain AWS-Region identisch sein.

    - Verwenden Sie die Tabelle mit den Tracking-Domains in Allgemeine AWS-Referenz , um die Tracking-Domain auszuwählen, die sich in derselben Region wie Ihre benutzerdefinierte Domain befindet.

> **Note**
>
> Abhängig von Ihrem Webhosting-Anbieter kann es einige Minuten dauern, bis die Änderungen, die Sie am DNS-Datensatz der Subdomäne vorgenommen haben, wirksam werden. Ihr Webhosting-Anbieter oder die IT-Organisation kann weitere Informationen zu diesen Verzögerungen bereitstellen.

Option 2: Konfigurieren einer HTTPS-Domäne

Sie können auch eine HTTPS-Domain verwenden, um geöffnete Klicks und Linkklicks zu verfolgen. Um eine HTTPS-Domain für die Nachverfolgung von Klicks auf geöffnete Inhalte und Links einzurichten, müssen Sie einige zusätzliche Schritte ausführen, die über die für die Einrichtung einer HTTP-Domain erforderlichen Schritte hinausgehen.

So richten Sie eine HTTPS-Subdomäne für die Verarbeitung von Öffnungs- und Klicklinks ein

1. Erstellen Sie eine Subdomäne zur Verwendung für Öffnungs- und Klicknachverfolgungs-Links. SES empfiehlt, dass diese Subdomain speziell für die Verarbeitung dieser Links vorgesehen ist und dass für jede versendete E-Mail, die AWS-Region Sie verfolgen möchten, eine Subdomain erstellt wird.
2. Überprüfen Sie die Subdomain für die Verwendung mit SES. Weitere Informationen finden Sie unter Erstellen einer Domänenidentität.
3. Erstellen Sie ein neues Konto bei einem Content Delivery Network (CDN) wie Amazon CloudFront, siehe Erste Schritte mit einer CloudFront Basisdistribution.
4. Konfigurieren Sie das CDN für den Ursprung, der die SES-Tracking-Domain ist, wie zum Beispiel `r.us-east-1.awstrack.me`. Das CDN muss auf die AWS Tracking-Domain verweisen, die sich in derselben Region wie Ihre benutzerdefinierte Domain befindet. Das CDN muss den vom Anforderer bereitgestellten `Host` Header an den Ursprung weitergeben. Weitere Informationen finden Sie in diesem AWS Re:POST-Artikel.

   - Verwenden Sie die Tabelle mit den Tracking-Domains in Allgemeine AWS-Referenz , um die Tracking-Domain auszuwählen, die sich in derselben Region wie Ihre benutzerdefinierte Domain befindet.
5. Wenn Sie Route 53 zur Verwaltung der DNS-Konfiguration für Ihre Domain und CloudFront als CDN verwenden, erstellen Sie in Route 53 einen Aliaseintrag, der auf Ihre CloudFront

Distribution verweist (z. B. d111111abcdef8.cloudfront.net). Für weitere Informationen sehe Sie Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole im Amazon Route 53-Entwicklerhandbuch.

Fügen Sie andernfalls in der DNS-Konfiguration für Ihre Subdomäne einen CNAME-Datensatz hinzu, der sich auf die Adresse Ihres CDN bezieht.

6. Erwerben Sie ein SSL-Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle. Das Zertifikat sollte sowohl die Subdomäne, die Sie in Schritt 1 erstellt haben, als auch das CDN, das Sie in Schritt 3 bis 5 konfiguriert haben, abdecken. Laden Sie das Zertifikat in das CDN hoch.
7. Sie können den folgenden curl-Befehl verwenden, um zu überprüfen, ob Ihre neu erstellte benutzerdefinierte Domain die richtige Region und das richtige HTTPS-Protokoll verwendet. Im folgenden Beispiel ist bis auf den Namen Ihrer Domain alles wörtlich:

```
curl --head https://custom.domain.com/favicon.ico
```

Eine Antwort wird wie im folgenden Beispiel zurückgegeben:

```
(python-sdk-test) jdoe@12a34567b89c BaconRedirectService % curl --head https://
custom.domain.com/favicon.ico
HTTPS/1.1 200 OK
x-amz-ses-region: us-east-1
x-amz-ses-request-protocol: https
Content-Type: image/x-icon
Transfer-Encoding: chunked
Date: Fri, 30 Aug 2024 13:50:14 GMT
```

Diese Antwort enthält die folgenden Eigenschaften:

- Der `x-amz-ses-region` Header-Wert ist die SES-Region, die die Anfrage erhalten hat.
- Der `x-amz-ses-request-protocol` Header-Wert ist das Protokoll, das für die Anfrage zwischen dem CDN und SES im Header verwendet wird.

Wenn Ihre Einrichtung korrekt ist, sollte die Region die Region widerspiegeln, in der Ihre Domain erstellt wurde, und das Protokoll sollte HTTPS sein.

Teil 2: Spezifizieren Sie Ihre benutzerdefinierte Weiterleitungsdomain und Ihre HTTPS-Richtlinie über einen Konfigurationssatz

Nachdem Sie Ihre Domain für die Verarbeitung von Weiterleitungen zum Öffnen und Klicken konfiguriert haben, müssen Sie Ihre benutzerdefinierte Domain und Ihre HTTPS-Richtlinie in einem Konfigurationssatz angeben.

Wenn Sie eine E-Mail mithilfe eines Konfigurationssatzes senden und dieser Konfigurationssatz für die Verwendung einer benutzerdefinierten Weiterleitungsdomäne konfiguriert ist, verwenden die Links zum Öffnen und Klicken in dieser E-Mail automatisch die im Konfigurationssatz angegebenen benutzerdefinierten Domänen- und HTTPS-Richtlinienoptionen.

Sie können dies mit der SES-Konsole oder dem `CreateConfigurationSet`v2-API-Vorgang abschließen.

So geben Sie mithilfe der Konsole eine benutzerdefinierte Umleitungsdomäne und eine HTTPS-Richtlinie an

- Verwenden Sie beim Erstellen oder Bearbeiten eines Konfigurationssatzes die Tracking-Optionen in Schritt 4 von, Erstellen Sie einen Konfigurationssatz. um Ihre benutzerdefinierte Weiterleitungsdomain und die HTTPS-Richtlinienoptionen anzugeben.

Um eine benutzerdefinierte Umleitungsdomäne und eine HTTPS-Richtlinie anzugeben, verwenden Sie den AWS CLI

Sie können den `CreateConfigurationSet`Vorgang in der SES-API v2 verwenden und die `TrackingOptions` Eigenschaft verwenden, um Ihre benutzerdefinierte Weiterleitungsdomäne und die HTTPS-Richtlinie anzugeben. Sie können diesen Vorgang von der aus aufrufen, AWS CLI wie im folgenden Beispiel gezeigt.

- Erstellen Sie den Konfigurationssatz AWS-Region dort, wo Sie E-Mails senden und verfolgen möchten:

```
aws sesv2 create-configuration-set --cli-input-json file://create.json
```

- In diesem Beispiel verwendet die Eingabedatei Parameter der `TrackingOptions`Eigenschaft. Sie `CustomRedirectDomain` gibt die benutzerdefinierte Domain an, die für die Nachverfolgung geöffneter und geklickter Links verwendet werden soll, und `HttpsPolicy` gibt eine HTTPS-Richtlinienoption an:

```
{
    "ConfigurationSetName": "my-config-set",
    "TrackingOptions": {
        "CustomRedirectDomain": "marketing.example.com",
        "HttpsPolicy": "REQUIRE"
    },
    "SendingOptions": {
        "SendingEnabled": true
    }
}
```

Für den `HttpsPolicy` Parameter können die folgenden Werte angegeben werden, um das Protokoll der Tracking-Links zum Öffnen und Klicken für Ihre benutzerdefinierte Weiterleitungsdomain festzulegen:

- `OPTIONAL`— (Standardverhalten) Offene Tracking-Links werden mit HTTP umschlossen. Links zur Klickverfolgung werden unter Verwendung des Originalprotokolls des Links umschlossen.
- `REQUIRE`— Links zum Öffnen und Klicken werden beide mit HTTPS umschlossen.
- `REQUIRE_OPEN_ONLY`— Offene Tracking-Links werden mit HTTPS umschlossen. Links zur Klickverfolgung werden unter Verwendung des Originalprotokolls des Links verpackt.

Teil 3: Spezifizierung der Ereignistypen „Öffnen“ und „Klicken“ mithilfe eines Konfigurationssatzes

Nachdem Sie Ihre benutzerdefinierte Domain und Ihre HTTPS-Richtlinie im Konfigurationssatz im vorherigen Schritt angegeben haben, müssen Sie and/or Open-Click-Ereignistypen angeben, die in einem Ereignisziel über einen Konfigurationssatz nachverfolgt werden sollen.

Sie können dies mit der SES-Konsole oder dem `CreateConfigurationSetEventDestination`v2-API-Vorgang abschließen.

and/or Klicken Sie in der Konsole auf Ereignistypen, um „Öffnen“ auszuwählen

- Geben Sie beim Erstellen oder Ändern eines Eventziels in Schritt 6 von die Option Öffnen und Klicken Sie auf Tracking anthe section called “Erstellen eines Ereignisziels”, um die Ereignistypen anzugeben.

Festlegen eines Konfigurationssatzes für das Senden von E-Mail

Zum Verwenden eines Konfigurationssatzes beim Senden von E-Mails müssen Sie den Namen des Konfigurationssatzes in den Headern der E-Mail übergeben. Alle E-Mail-Versandmethoden von Amazon SES — einschließlich der SMTP-Schnittstelle AWS CLI, der und der Amazon SES SMTP-Schnittstelle — ermöglichen es Ihnen AWS SDKs, einen Konfigurationssatz in den Headern der von Ihnen gesendeten E-Mail zu übergeben.

Wenn Sie die SMTP-Schnittstelle oder die `SendRawEmail` API-Operation nutzen, können Sie einen Konfigurationssatz angeben, indem Sie den folgenden Header in Ihre E-Mail einschließen (und so *`ConfigSet`* durch den Namen des Konfigurationssatzes ersetzen, den Sie verwenden möchten):

```
X-SES-CONFIGURATION-SET: ConfigSet
```

Dieses Handbuch enthält Codebeispiele für das Senden von E-Mails über die AWS SDKs und die Amazon SES SMTP-Schnittstelle. Jedes dieser Beispiele enthält eine Methode für das Festlegen eines Konfigurationssatzes. Die step-by-step Verfahren zum Senden von E-Mails, die Verweise auf Konfigurationssätze enthalten, finden Sie im Folgenden:

- Senden von E-Mails über Amazon SES mithilfe eines AWS SDK
- Verwenden der Amazon-SES-SMTP-Schnittstelle zum Senden von E-Mails

Reputationsmetriken anzeigen und exportieren

Amazon SES exportiert automatisch Informationen über die allgemeinen Absprungs- und Beschwerdequoten für Ihr gesamtes Konto an Amazon CloudWatch. Sie können diese Metriken verwenden CloudWatch, um Alarme zu erstellen oder den E-Mail-Versand mithilfe einer Lambda-Funktion automatisch anzuhalten.

Außerdem können Sie Zuverlässigkeitsmetriken für einzelne Konfigurationssätze nach CloudWatch exportieren. Mit dem Exportieren von Zuverlässigkeitsdaten auf der Ebene des Konfigurationssatzes erhalten Sie mehr Kontrolle über Ihre Absenderzuverlässigkeit.

Dieser Abschnitt enthält Verfahren zum Exportieren von Reputationsdaten für einzelne Konfigurationssätze CloudWatch mithilfe der Amazon SES SES-API.

Aktivieren des Exports von Reputationsmetriken

Um mit dem Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz zu beginnen, verwenden Sie die `UpdateConfigurationSetReputationMetricsEnabled`-API-Operation. Für den Zugriff auf die Amazon SES SES-API empfehlen wir die Verwendung der AWS CLI oder einer der AWS SDKs.

Bei diesem Verfahren AWS CLI wird davon ausgegangen, dass der auf Ihrem Computer installiert und ordnungsgemäß konfiguriert ist. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

So aktivieren Sie den Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws ses update-configuration-set-reputation-metrics-enabled --configuration-set-
  name ConfigSet --enabled
  ```

  Ersetzen Sie *`ConfigSet`* den vorherigen Befehl durch den Namen des Konfigurationssatzes, für den Sie mit dem Export von Reputationsmetriken beginnen möchten.

Deaktivieren des Exports von Reputation-Metriken

Sie können auch die `UpdateConfigurationSetReputationMetricsEnabled`-API-Operation verwenden, um den Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz zu deaktivieren.

So deaktivieren Sie den Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws ses update-configuration-set-reputation-metrics-enabled --configuration-set-
  name ConfigSet --no-enabled
  ```

  Ersetzen Sie *`ConfigSet`* den vorherigen Befehl durch den Namen des Konfigurationssatzes, für den Sie den Export von Reputationsmetriken deaktivieren möchten.

Verwendung globaler Endpunkte in Amazon SES

Amazon SES Global Endpoints ist eine Funktion, die die Kontinuität und Zuverlässigkeit Ihrer E-Mail-Versandvorgänge verbessert. Dieses Kapitel führt Sie durch das Konzept, die Einrichtung und die Nutzung globaler Endgeräte und hilft Ihnen dabei, Multi-Region-Sending (MRS) zu nutzen, um eine höhere Verfügbarkeit und verbesserte Disaster-Recovery-Funktionen für Ihre E-Mail-Workloads zu erreichen.

Was sind globale Endgeräte?

Globale Endpunkte sind Ressourcen, mit denen Sie Ihre ausgehenden SES-Workloads auf zwei verteilen können. AWS-Regionen Nach der Konfiguration teilt SES Ihren Sendeverkehr automatisch zwischen den ausgewählten primären und sekundären Regionen auf. Sollte es in einer der Regionen zu Beeinträchtigungen kommen, leitet SES den Verkehr automatisch von der betroffenen Region weg, um die Kontinuität Ihres Sendebetriebs aufrechtzuerhalten.

Zu den wichtigsten Vorteilen der Verwendung globaler Endgeräte gehören:

- Verbesserte Kontinuität beim E-Mail-Versand
- Automatischer Failover zwischen Regionen
- Vereinfachte Konfiguration mit mehreren Regionen

So funktionieren globale Endgeräte

Wenn Sie einen globalen Endpunkt einrichten, wählen Sie eine primäre Region (in der der Endpunkt erstellt wird) und eine sekundäre Region aus. SES erstellt dann einen multiregionalen Endpunkt (MREP), der als Einstiegspunkt für Ihre E-Mail-Versandanfragen dient.

Der globale Endpunkt-Setup-Prozess synchronisiert wichtige Artefakte und Sendelimits von Ihrer primären Region mit Ihrer sekundären Region. Dadurch wird sichergestellt, dass beide Regionen über gleichwertige verifizierte Identitäten, Konfigurationssätze und genehmigte Sendelimits verfügen, die für das gesamte erwartete Volumen ausreichend sind.

Sobald der globale Endpunkt bereit ist und seine Endpunkt-ID im SendEmail API-Aufruf angegeben wurde, leitet SES Ihren ausgehenden Datenverkehr automatisch zwischen Ihrer primären und sekundären Region weiter. Wenn eine Region beeinträchtigt wird, wird der Verkehr von dieser Region weg in die andere Region gewichtet, bis die Beeinträchtigung behoben ist.

Einrichtung globaler Endpunkte

Themen

- Voraussetzungen
- Einen globalen Endpunkt erstellen
- Globale Endpunktstaaten

Voraussetzungen

Bevor Sie einen globalen Endpunkt erstellen, müssen Sie SES zunächst die Erlaubnis erteilen, serviceverknüpfte Rollen (SLRs) in Ihrem Konto zu erstellen. Diese Rollen ermöglichen wichtige Servicefunktionen und den Zugriff auf Ressourcen, die für die Erstellung, Nutzung und Überwachung globaler Endgeräte erforderlich sind. Dies kann durch die Implementierung der folgenden Richtlinie erreicht werden:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "ses.amazonaws.com"
        }
      }
    }
  ]
}
```

Einen globalen Endpunkt erstellen

So erstellen Sie einen neuen globalen Endpunkt:

1. Öffnen Sie die SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich Global Endpoints aus.
3. Wählen Sie Create Global Endpoint aus und geben Sie einen Namen in das Feld Name ein.
4. Wählen Sie im Dropdownmenü eine sekundäre Region aus. (Ihre primäre Region ist standardmäßig die Region, mit der Sie sich bei der Konsole angemeldet haben.)
5. (Optional) Fügen Sie Ihrem globalen Endpunkt ein oder mehrere Tags hinzu.
6. Überprüfen Sie die Konfiguration und wählen Sie Create Global Endpoint aus.

Der Erstellungsvorgang kann einige Sekunden dauern. Sobald der Vorgang abgeschlossen ist, ändert sich der Status Ihres globalen Endpunkts auf „Bereit“.

Verwenden von AWS CLI:

```
aws sesv2 create-multi-region-endpoint --primary-region us-west-2 --secondary-
region us-east-1 --endpoint-name MyGlobalEndpoint
```

Für das obige Beispiel gilt:

- *us-west-2*Ersetzen Sie es durch die primäre Region für Ihren globalen Endpunkt.
- *us-east-1*Ersetzen Sie es durch die sekundäre Region für Ihren globalen Endpunkt.
- *MyGlobalEndpoint*Ersetzen Sie es durch den benutzerfreundlichen Namen, um Ihren globalen Endpunkt zu erhalten.

Globale Endpunktstaaten

Globale Endpunkte können die folgenden Status haben:

- Erstellen — Die Ressource wird bereitgestellt
- Bereit — Die Ressource ist einsatzbereit
- Fehlgeschlagen — Die Ressource konnte nicht bereitgestellt werden
- Löschen — Die Ressource wird wie angefordert gelöscht

Die sekundäre Region wird vorbereitet

Nachdem Sie Ihren globalen Endpunkt erstellt haben, müssen Sie nun sicherstellen, dass Ihre E-Mail-Versandkonfiguration, einschließlich all ihrer Komponenten (Identitäten, Konfigurationssätze, E-Mail-Vorlagen und Sendelimits), in den primären und sekundären Regionen konsistent ist, bevor Sie den globalen Endpunkt zum Senden von E-Mails verwenden. Diese Ausrichtung ist entscheidend, um potenzielle Probleme zu vermeiden und die ordnungsgemäße Zustellung und Nachverfolgung von E-Mails sicherzustellen.

Die Funktion zur Regionsduplizierung in der Konsole unterstützt Sie dabei, Ressourcen automatisch zu duplizieren und Einstellungen auf Kontoebene von der primären in die sekundäre Region zu duplizieren. So können Sie schnell sicherstellen, dass beide Regionen über gleichwertige Konfigurationen verfügen.

Aufgrund der Ressourcenabhängigkeiten ist die Reihenfolge, in der Sie Ressourcen duplizieren, von Bedeutung. Um Konflikte zu vermeiden, halten Sie sich an die folgende Reihenfolge der Themen:

Themen

- Konfigurationssätze duplizieren
- Verifizierte Domänenidentitäten duplizieren
- Duplizierung von Produktionslimits

Konfigurationssätze duplizieren

Sie können mehrere Konfigurationssätze aus Ihrer primären Region auswählen, die zusammen mit ihren Einstellungen in der sekundären Region dupliziert werden sollen.

Die Funktion „Konfigurationssätze duplizieren“ ermöglicht Ihnen:

- Duplizieren Sie mehrere Konfigurationssätze gleichzeitig in die sekundäre Region.
- Prüfen Sie, ob es Unterschiede zwischen den Konfigurationssätzen in der primären Region und der sekundären Region gibt.

So duplizieren Sie Konfigurationssätze:

1. Wählen Sie auf der Seite Globale Endpunkte den globalen Endpunkt aus, den Sie duplizieren möchten, indem Sie ihn in der Spalte Name auswählen.

2. Erweitern Sie auf der Karte Doppelte Konfigurationssätze den Bereich Aktionen für Konfigurationssätze und wählen Sie Duplizieren aus.
3. Wählen Sie bis zu 10 Konfigurationssätze aus, gefolgt von Bestätigen.
4. Wenn der Status nicht erfolgreich ist, wählen Sie Bericht anzeigen, um das Problem zu identifizieren.
5. (Optional) Bei zuvor duplizierten Konfigurationssätzen können Sie nach Unterschieden zwischen der primären und der sekundären Region suchen, indem Sie die Option Unterschiede prüfen auswählen und dabei die letzten drei Schritte wiederholen.

> **Note**
>
> - Wenn der von Ihnen duplizierte Konfigurationssatz Ereignisziele, Reputationsoptionen oder Archivierungsoptionen enthält oder in einer E-Mail-Vorlage referenziert wird, müssen diese Einstellungen in der sekundären Region manuell konfiguriert werden.
> - Wenn Sie die Archivierung für gesendete (ausgehende) E-Mails in einer Konfiguration in der primären Region aktiviert haben, müssen Sie die Archivierung für gesendete (ausgehende) E-Mails im Konfigurationssatz der sekundären Region manuell aktivieren, indem Sie ein Archiv verwenden, das in der sekundären Region mit demselben Namen erstellt wurde.

Verifizierte Domänenidentitäten duplizieren

Um sicherzustellen, dass die globale Endpunktkonfiguration effektiv funktioniert, muss Ihre Absenderdomänenidentität sowohl in der primären als auch in der sekundären Region überprüft werden. SES verwendetDeterministisches einfaches DKIM (DEED), um diesen Prozess zu vereinfachen.

Deterministic Easy DKIM (DEED) ist eine Funktion, die konsistente DKIM-Token für alle generiert, die auf einer übergeordneten Domain AWS-Regionen basieren, die mit Easy DKIM konfiguriert ist. Diese Konsistenz ermöglicht es SES, eine Domain in der sekundären Region automatisch zu verifizieren, sobald sie in der primären Region verifiziert wurde, ohne dass zusätzliche Aktualisierungen der DNS-Einträge erforderlich sind. Daher müssen Sie sicherstellen, dass die Domänenidentität, die Sie duplizieren möchten, d. h. die übergeordnete Identität, bereits mit Easy DKIM konfiguriert ist.

Die Funktion „Verifizierte Domänenidentitäten duplizieren“ ermöglicht Ihnen:

- Duplizieren Sie mehrere Domain-Identitäten gleichzeitig in die sekundäre Region.
- Verifizieren Sie sie automatisch mit Deterministic Easy DKIM (DEED).
- Suchen Sie nach Unterschieden zwischen Identitäten in der primären Region und der sekundären Region.

So duplizieren Sie Identitäten von der SES-Konsole aus:

1. Wählen Sie auf der Seite Globale Endgeräte den globalen Endpunkt aus, den Sie duplizieren möchten, indem Sie ihn in der Spalte Name auswählen.
2. Erweitern Sie auf der Karte Doppelte verifizierte Domänenidentitäten den Bereich Identitätsaktionen und wählen Sie Duplizieren aus.
3. Wählen Sie bis zu 10 Identitäten aus, gefolgt von Bestätigen.
4. Wenn der Status nicht erfolgreich ist, wählen Sie Bericht anzeigen, um das Problem zu identifizieren.
5. (Optional) Bei bereits duplizierten Identitäten können Sie nach Unterschieden zwischen der primären und der sekundären Region suchen, indem Sie die Option Unterschiede überprüfen auswählen und dabei die letzten drei Schritte wiederholen.

> **Note**
>
> - Mit BYODKIM verifizierte oder selbstsignierte Domänenidentitäten müssen in der sekundären Region manuell erstellt werden, da DEED in diesem Fall nicht anwendbar ist.
> - Für Domänenidentitäten, die E-Mail-Absender-Attribute, Richtlinien oder Feedback-Weiterleitung und Benachrichtigungen verwenden, müssen diese Funktionen in der sekundären Region manuell konfiguriert werden.

Duplizierung von Produktionslimits

SES prüft, ob die Sendelimits zwischen den Regionen übereinstimmen, und ermöglicht es Ihnen, bei Bedarf Limiterhöhungen in der sekundären Region zu beantragen.

Die Funktion „Produktionslimits duplizieren“ ermöglicht Ihnen:

- Prüfen Sie, ob die Produktionsgrenzen zwischen primären und sekundären Regionen aufeinander abgestimmt sind.
- Beantragen Sie bei Bedarf eine Erhöhung der Grenzwerte in der sekundären Region.

Um Produktionslimits zu duplizieren:

1. Wählen Sie auf der Seite Globale Endpunkte den globalen Endpunkt aus, den Sie duplizieren möchten, indem Sie ihn in der Spalte Name auswählen.
2. Wenn auf der Karte Doppelte Produktionslimits angezeigt wird, dass der Status Versandlimits nicht abgestimmt ist, erweitern Sie den Bereich Aktionen für Versandlimits.
3. Wählen Sie Sendelimits für die sekundäre Region verwalten aus.
4. Die Seite „Service Quotas“ wird in der sekundären Region geöffnet, auf der Sie eine Erhöhung der „Versandquote“ und der „Versandrate“ beantragen können, um sie an die Werte der primären Region anzupassen.

   > **Tip**
   >
   > Es wird empfohlen, dass Sie das maximale Kontingent beantragen, für das Sie in beiden Regionen berechtigt sind. Während der E-Mail-Verkehr unter normalen Betriebsbedingungen auf beide Regionen verteilt wird, wird bei einem Failover-Ereignis der gesamte E-Mail-Verkehr an eine Region gesendet, und die Grenzwerte sollten ausreichen, um das gesamte Volumen zu bewältigen.

5. (Optional) Sie können auch Produktionserhöhungen für Ihre primäre Region beantragen, indem Sie Sendebeschränkungen für die primäre Region verwalten auswählen und gleichzeitig die beiden vorherigen Schritte wiederholen.

> **Important**
>
> Es ist wichtig, dass beide Regionen über die gleichen verifizierten Identitäten und Konfigurationssätze verfügen, mit denen Sie E-Mails versenden möchten, und dass die Sendelimits übereinstimmen, um die ordnungsgemäße Funktionalität des globalen Endpunkts sicherzustellen. Jede Diskrepanz könnte zu Zustellungsfehlern, verminderter Ausfallsicherheit und fehlenden Metriken führen.

Verwendung globaler Endpunkte

Themen

- Integrieren in Ihre Anwendung
- Überwachung und Metriken

Integrieren in Ihre Anwendung

Wenn Sie einen globalen Endpunkt in Ihrer Anwendung verwenden, müssen Sie dessen Endpunkt-ID abrufen.

So rufen Sie die Endpunkt-ID eines globalen Endpunkts ab:

1. Rufen Sie in der SES-Konsole die Seite Globale Endgeräte auf und wählen Sie den globalen Endpunkt aus, den Sie verwenden möchten, indem Sie ihn in der Spalte Name auswählen.
2. Wählen Sie auf der Seite mit den globalen Endpunktdetails unter Endpunkt-ID das Kopiersymbol aus.

Verwenden von AWS CLI:

```
aws sesv2 get-multi-region-endpoint --endpoint-name MyGlobalEndpoint --region us-west-2
```

Für das obige Beispiel gilt:

- *MyGlobalEndpoint*Ersetzen Sie es durch den benutzerfreundlichen Namen, den Sie Ihrem globalen Endpunkt bei der Erstellung gegeben haben.
- *us-west-2*Ersetzen Sie es durch die primäre Region, in der Sie Ihren globalen Endpunkt erstellt haben.
- Die API-Antwort wird den Wert Ihrer Endpunkt-ID enthalten, `"EndpointId": "abcdef12.g3h"` z. B.

Sobald Sie die Endpunkt-ID Ihres globalen Endpunkts erhalten haben, können Sie Ihre Aufrufe `SendEmail`oder `SendBulkEmail`API-Aufrufe so aktualisieren, dass sie den Endpunkt-ID-Wert für den `endpoint-id` Parameter enthalten. Hier ist ein Beispiel dafür, wie Sie die Endpunkt-ID in einem SendEmail API-Aufruf angeben, indem Sie AWS CLI:

```
aws sesv2 send-email \
                --from-email-address "sender@example.com" \
                --destination "ToAddresses=recipient@example.com" \
                --content "Subject={Data=Test
 email,Charset=UTF-8},Body={Text={Data=This is a test email sent using Amazon SES
 Global endpoints.,Charset=UTF-8}}" \
                --endpoint-id "abcdef12.g3h"
```

*abcdef12.g3h*Ersetzen Sie sie durch die tatsächliche Endpunkt-ID, die Sie entweder über die Konsole oder die API erhalten haben.

Überwachung und Metriken

Die Funktion Global Endpoints bietet einen einheitlichen Überblick über Ihr E-Mail-Versandvolumen sowohl in der primären als auch in der sekundären Region. Sie können auf diese Messwerte über den Tab Regionalübergreifende Metriken auf der Seite mit den globalen Endpunktdetails in der SES-Konsole zugreifen.

So greifen Sie auf Sendemetriken in beiden Regionen zu:

1. Rufen Sie in der SES-Konsole die Seite Globale Endgeräte auf und wählen Sie den globalen Endpunkt aus, für den Sie Messwerte anzeigen möchten, indem Sie ihn in der Spalte Name auswählen.
2. Wählen Sie auf der Seite mit den globalen Endpunktdetails den Tab Regionalübergreifende Metriken aus und geben Sie einen Zeitraum von bis zu 31 Tagen ein. Metriken für beide Regionen werden für den angegebenen Zeitraum angezeigt.

Mit dem AWS CLI:

```
aws cloudwatch get-metric-statistics \
                --namespace AWS/SES \
                --metric-name SendCount \
                --dimensions Name=ses:multi-region-endpoint-id,Value=abcdef12.g3h \
                --start-time 2024-10-01T00:00:00Z \ --end-time 2024-10-31T23:59:59Z \
                --period 86400 \
                --statistics Sum
```

*abcdef12.g3h*Ersetzen Sie es durch Ihre tatsächliche Endpunkt-ID.

Bewährte Methoden und Überlegungen

Die Einhaltung dieser bewährten Verfahren und Überlegungen trägt dazu bei, eine effektive Nutzung, Überwachung und Kostenoptimierung von globalen Endpunkten über mehrere AWS-Regionen Endgeräte hinweg sicherzustellen und so die Verfügbarkeit und Zuverlässigkeit der E-Mail-Versandfunktionen zu verbessern.

- Synchronisieren Sie regelmäßig alle Änderungen, die an Artefakten (z. B. Konfigurationssätzen, verifizierte Identitäten) zwischen den Regionen vorgenommen wurden, um die Integrität des Versands aufrechtzuerhalten.
- Überwachen Sie die regionsübergreifenden Metriken, um eine ausgewogene Verteilung des Datenverkehrs sicherzustellen und potenzielle Probleme zu identifizieren.
- Beachten Sie, dass globale Endgeräte zwar eine verbesserte Verfügbarkeit bieten, den physischen Status der regionalen Verfügbarkeit von SES Outbound jedoch nicht ändern.
- Beachten Sie, dass globale Endpunkte beim Start keinen SMTP- oder VPC-Endpunktzugriff unterstützen.
- Berücksichtigen Sie mögliche Gebühren für ausgehenden Datenverkehr, wenn Sie ein AWS Gateway für die Adressübersetzung verwenden.
- Beachten Sie, dass die API-Latenz bei Aufrufen in MREP-fähige entfernte Regionen geringfügig ansteigen kann.

Preisgestaltung

Die genauen Preisangaben können sich zwar ändern, aber es wird davon ausgegangen, dass bei globalen Endpunkten für das gleiche Postvolumen ein Preisaufschlag gegenüber dem Versand in einer einzelnen Region anfällt. Trotz dieses Anstiegs wird davon ausgegangen, dass die Gesamtkosten im Vergleich zu anderen E-Mail-Dienstanbietern wettbewerbsfähig bleiben werden.

Die meisten up-to-date Preisinformationen finden Sie auf der Amazon SES SES-Preisseite.

Verwenden dedizierter IP-Adressen mit Amazon SES

Wenn Sie ein neues Amazon-SES-Konto erstellen, werden Ihre E-Mails standardmäßig von IP-Adressen gesendet, die mit anderen SES-Benutzern gemeinsam genutzt werden. Sie können auch dedizierte IP-Adressen verwenden, die für Ihre ausschließliche Nutzung reserviert sind, indem Sie sie gegen eine zusätzliche Gebühr leasen. Damit erhalten Sie die vollständige Kontrolle über Ihre Reputation als Absender und können Ihre Reputation für verschiedene Segmente innerhalb von E-Mail-Programmen isolieren. Amazon SES bietet zwei Möglichkeiten zur Bereitstellung und Verwaltung einer dedizierten IP-Adresse:

- Standard – Bezieht sich auf dedizierte IP-Adressen, die Sie manuell einrichten und verwalten, einschließlich der Option, sie manuell aufzuwärmen und zu skalieren sowie sie manuell in oder aus IP-Pools zu verschieben. (Diese wurden in SES zuvor als dedizierte IP-Adressen bezeichnet.)
- Verwaltet – Bezieht sich auf dedizierte IP-Adressen, die von SES automatisch in Ihrem Namen eingerichtet werden, um eine schnelle und einfache Möglichkeit zu bieten, dedizierte IP-Adressen zu verwenden, die von SES verwaltet werden. Sie werden automatisch für jeden ISP einzeln aufgewärmt und basierend auf Ihrem Sendevolumen skaliert. Damit wird sichergestellt, dass Ihre dedizierten IP-Adressen optimal auf Ihr Sendeverhalten von E-Mails abgestimmt sind.

Wenn Sie sich zwischen gemeinsam genutzten IP-Adressen oder den beiden oben definierten Arten der dedizierten IP-Adressen entscheiden, wählen Sie diejenigen aus, die die meisten Vorteile im Hinblick auf Typ, Volumen und Muster der von Ihnen gesendeten E-Mails bieten. Als Entscheidungshilfe sind diese Vorteile in der folgenden Tabelle zusammengefasst. Wählen Sie einen Artikel in der Spalte Benefit (Vorteil) aus, um weitere Informationen zu erhalten.

Vorteil	Gemeinsame IP-Adressen	Dedizierte IP-Adressen (Standard)	Dedizierte IP-Adressen (verwaltet)
Sofort einsatzbereit	Ja	Nein	Nein
Zusätzliche Einrichtung erforderlich	Nein	Ja	Ja
IP-Adressen und Reputation isoliert von anderen SES-Kunden	Nein	Ja	Ja

Vorteil	Gemeinsame IP-Adressen	Dedizierte IP-Adressen (Standard)	Dedizierte IP-Adressen (verwaltet)
Die Kapazität steigt automatisch, wenn der Verkehr zunimmt	Nein	Nein	Ja
Geeignet für Kunden mit kontinuierlichen, planbaren Versandmustern	Ja	Ja	Ja
Geeignet für Kunden mit weniger planbaren Versandmustern	Ja	Nein	Ja
Geeignet für Versender von großen Volumen	Ja	Ja	Ja
Geeignet für Versender von geringem Volumen	Ja	Nein	Nein
Zusätzliche monatliche Kosten	Nein	Ja	Ja
Vollständige Kontrolle über die Reputation des Absenders	Nein	Ja	Ja
Isolierung der Reputation nach E-Mail-Typ, Empfänger oder anderen Faktoren	Nein	Ja	Ja

Vorteil	Gemeinsame IP-Adressen	Dedizierte IP-Adressen (Standard)	Dedizierte IP-Adressen (verwaltet)
Stellt bekannte IP-Adressen zur Verfügung, die sich nie ändern.	Nein	Ja	Nein

> **Important**
>
> Wenn Sie nicht vorhaben, regelmäßig und geplant große Mengen an E-Mails zu versenden, empfehlen wir Ihnen, gemeinsam genutzte IP-Adressen zu verwenden. Wenn Sie in Situationen, in denen Ihre Sendemuster sehr unregelmäßig sind, dedizierte IP-Adressen verwenden möchten, ist die Verwendung von Dedicated IPs (verwaltet) die bessere Option.

Einfache Einrichtung

Gemeinsam genutzte IP-Adressen – Sie müssen keine zusätzliche Konfiguration vornehmen. Ihr SES-Konto kann E-Mails senden, sobald Sie eine E-Mail-Adresse verifizieren und aus der Sandbox verschieben.

Dedizierte IP-Adressen (Standard) — Sie müssen eine Anfrage über das AWS Support Center einreichen und optional dedizierte IP-Pools konfigurieren.

Dedizierte IP-Adressen (verwaltet) – Sie müssen keine Anfrage für dedizierte IP-Adressen stellen. Sie werden automatisch zugewiesen, wenn Sie sich anmelden und die Anleitung zum Erstellen Ihres verwalteten dedizierten Pools einmalig befolgen.

Reputationsverwaltung

Die Reputation von IP-Adressen basiert größtenteils auf historischen Versandmustern und -volumen. Eine IP-Adresse, die über einen langen Zeitraum hinweg konsistente Mengen an E-Mails versendet, hat in der Regel eine gute Reputation.

Gemeinsam genutzte IP-Adressen – Diese Adressen werden von mehreren SES-Kunden gemeinsam genutzt und senden gemeinsam eine große Menge an E-Mails. AWS verwaltet den ausgehenden Datenverkehr sorgfältig, um die Reputation der gemeinsam genutzten IP-Adressen zu maximieren.

Dedizierte IP-Adressen (Standard) — Nach dem Aufwärmen werden Ihre IP-Adressen vom gemeinsam genutzten SES-Pool isoliert und Sie behalten Ihren eigenen Ruf als Absender, indem Sie konsistente und vorhersehbare E-Mail-Mengen versenden.

> **Note**
>
> Informationen zu Smart Network Data Services (SNDS) -Daten für Ihre dedizierten Geräte IPs (Standard) finden Sie unter. SNDS-Metriken für dedizierte IPs

Dedizierte IP-Adressen (verwaltet) — nach dem Aufwärmen Ihrer neuen IPs Adressen werden sie vom gemeinsam genutzten SES-Pool isoliert und Sie behalten Ihren eigenen Ruf als Absender. Der zusätzliche Vorteil besteht darin, dass Sie die Reputation jedes Internetdienstanbieters verfolgen und ausgehende Sendungen entsprechend optimal planen können. Während Sie also Ihre Reputation als Absender beibehalten, trägt diese Automatisierung dazu bei, die allgemeine Zustellbarkeit zu verbessern und die Unzustellbarkeitsraten im Vergleich zu gleichwertigen Workloads auf manuell konfigurierten dedizierten IP-Adressen zu reduzieren.

Planbarkeit von Sendemustern

Eine IP-Adresse mit einer konsistenten Historie beim E-Mail-Versand hat eine bessere Reputation als eine, die plötzlich große Mengen an E-Mails ohne vorherige Sendehistorie versendet.

Gemeinsam genutzte IP-Adressen – Diese Option eignet sich für E-Mail-Versandmuster, die keinem vorhersehbaren Muster folgen. Mit gemeinsam genutzten IP-Adressen können Sie Ihre E-Mail-Versandmuster entsprechend der Situation erhöhen oder verringern.

Dedizierte IP-Adressen (Standard) – Sie müssen diese Adressen aufwärmen, indem Sie die Menge der versendeten E-Mails jeden Tag erhöhen. Der Prozess der "Einführung" neuer IP-Adressen ist in Aufwärmen dedizierter IP-Adressen (Standard) beschrieben. Sobald Ihre dedizierten IP-Adressen eingeführt sind, müssen Sie ein konsistentes Sendeverhalten beibehalten.

Dedizierte IP-Adressen (verwaltet) — Ihre dedizierten IP-Adressen werden automatisch für jede IP im verwalteten Pool aufgewärmt. Dabei wird eine adaptive Aufwärmstrategie (in Verbindung mit dem gemeinsam genutzten SES-Pool) verwendet, die die tatsächlichen Sendemuster berücksichtigt,

um das Warmup für jeden ISP individuell zu optimieren. Der verwaltete IP-Pool wird je nach ISP automatisch skaliert, je nach Nutzung und Berücksichtigung der ISP-spezifischen Richtlinien.

Volumen ausgehender E-Mails

Gemeinsam genutzte IP-Adressen – Diese Option ist am besten für Kunden geeignet, die nur geringe Mengen an E-Mails versenden.

Dedizierte IP-Adressen (Standard) | Dedizierte IP-Adressen (verwaltet) – Beide Optionen sind für Kunden geeignet, die große Mengen an E-Mails versenden. Die meisten verfolgen die Reputation einer bestimmten IP-Adresse ISPs nur dann, wenn sie eine beträchtliche Menge an E-Mails von dieser Adresse erhalten. Für jeden ISP, bei dem Sie sich eine Reputation aufbauen wollen, sollten Sie innerhalb von 24 Stunden mindestens einmal im Monat mehrere hundert E-Mails versenden. In einigen Fällen können beide Arten von dedizierten IP-Adressen auch für kleinere E-Mail-Mengen funktionieren. Beispielsweise können sie gut funktionieren, wenn Sie an eine kleine, genau definierte Gruppe von Empfängern senden, deren Mailserver E-Mails annehmen oder ablehnen, indem sie mit einer Liste mit bestimmten IP-Adressen statt der Reputation der IP-Adresse arbeiten.

Weitere Kosten

Gemeinsam genutzte IP-Adressen – Die Verwendung dieser IP-Adressen ist im regulären SES-Preis inbegriffen.

Dedizierte IP-Adressen (Standard) – Diese IP-Adressen sind gegen eine zusätzliche monatliche Gebühr pro geleaster IP-Adresse erhältlich. Informationen zur Preisgestaltung finden Sie auf der Seite SES – Preise.

Dedizierte IP-Adressen (verwaltet) — sind gegen eine monatliche Standardgebühr (unabhängig von der IPs benötigten Menge) und gegen eine Nutzungsgebühr pro Nachricht erhältlich. Informationen zur Preisgestaltung finden Sie auf der Seite SES – Preise.

Kontrolle über die Senderzuverlässigkeit

Gemeinsam genutzte IP-Adressen – Ihre Absenderreputation wird von SES kontrolliert.

Dedizierte IP-Adressen (Standard) | Dedizierte IP-Adressen (verwaltet) – Ihre Absenderreputation obliegt vollständig Ihrer Kontrolle. Ihr SES-Konto ist das einzige, das in der Lage ist, E-Mails von diesen Adressen aus zu versenden. Aus diesem Grund wird die Reputation des Absenders durch

Ihre E-Mail-Versandpraktiken bestimmt. Darüber hinaus überwacht eine dedizierte IPs (verwaltete) Lösung aktiv die ausgehenden IP-Adressen, die für den E-Mail-Versand verwendet werden. Dabei werden IP-Adressen mit der höchsten Leistung verwendet, um die E-Mail-Zustellung an Ihre Empfänger zu verbessern. Nutzungsdaten können mithilfe zusätzlicher Services wie CloudWatch Amazon-Metriken und der integrierten Dashboards in Amazon SES angezeigt werden.

Möglichkeit zur Isolierung der Senderzuverlässigkeit

Gemeinsam genutzte IP-Adressen – Ihre Absenderreputation wird auf Kontoebene festgelegt und kann nicht isoliert werden.

Dedizierte IP-Adressen (Standard) | Dedizierte IP-Adressen (verwaltet) – Sie können Ihre Reputationsmetriken für verschiedene Komponenten innerhalb Ihres E-Mail-Programms isolieren, indem Sie dedizierte IP-Pools erstellen. Hierbei handelt es sich um Gruppen von dedizierten IP-Adressen, die für den Versand bestimmter E-Mail-Typen verwendet werden können. Beispielsweise können Sie einen Pool von dedizierten IP-Adressen für den Versand von Marketing-E-Mails und einen weiteren Pool für den Versand von Transaktions-E-Mails erstellen.

Bekannte, unveränderliche IP-Adressen

Gemeinsam genutzte IP-Adressen – Sie kennen die von SES zum Versenden Ihrer E-Mails verwendeten IP-Adressen nicht. Diese können sich jederzeit ändern.

Dedizierte IP-Adressen (Standard) — Die Werte der Adressen, an die Ihre E-Mails gesendet werden, finden Sie auf der IPs Seite Dediziert der SES-Konsole. Dies liegt daran, dass dedizierte IP-Adressen statisch sind.

Dedizierte IP-Adressen (verwaltet) – SES konfiguriert automatisch die optimale Anzahl dedizierter IP-Adressen basierend auf Ihren Sendemustern. Während SES die automatische Skalierung Ihres IP-Pools verwaltet, können Sie alle dedizierten IP-Adressen, die Ihrem Konto derzeit zugewiesen sind, über die SES-Konsole oder API einsehen. Die Anzahl der IPs in Ihrem Pool wird je nach Sendeanforderung weiterhin dynamisch steigen oder sinken.

Dedizierte IP-Adressen (Standard) in Amazon SES

Dedizierte IP-Adressen (Standard) sind dedizierte IP-Adressen, die Sie in SES manuell einrichten und verwalten. Sie unterscheiden sich von denen, die mit der SES-Funktion the section called “Dedizierte IP-Adressen (verwaltet)” automatisch eingerichtet und verwaltet werden. Dedicated IPs

(Standard) ermöglicht Ihnen nicht nur die volle Kontrolle über Ihre Senderreputation mithilfe von dedizierten IP-Adressen, sondern ermöglicht Ihnen auch die vollständige Verwaltung Ihrer dedizierten Adressen IPs, einschließlich Aufwärmen, Skalierung und IP-Poolverwaltung.

Dedicated IPs (Standard) und Dedicated IPs (verwaltet) beziehen sich beide auf dedizierte IP-Adressen, die Sie gegen Aufpreis in SES leasen, sich jedoch in der Art und Weise unterscheiden, wie sie implementiert und verwaltet werden. Es gibt zwar Vorteile, die beiden gemeinsam sind, aber sie bieten je nach Art des E-Mail-Versands einzigartige Vorteile, wie unter Dedizierte IP-Adressen beschrieben.

In den Themen dieses Abschnitts wird erklärt, wie Sie dediziert IPs (Standard) in SES manuell einrichten und verwalten.

Themen

- Anfordern und Freigeben dedizierter IP-Adressen (Standard)
- Aufwärmen dedizierter IP-Adressen (Standard)
- Erstellung von standardmäßigen dedizierten IP-Pools für dedizierte IPs (Standard)

Anfordern und Freigeben dedizierter IP-Adressen (Standard)

Wenn Sie dedizierte IP-Adressen (Standard) verwenden möchten, müssen Sie diese zuerst anfordern. Wenn Sie sie nicht mehr benötigen, müssen Sie sie freigeben. Dedizierte IPs (Standard) über das Center anfragen und aufgeben.AWS Support Wir berechnen Ihrem Konto für jede dedizierte Standard-IP-Adresse, die Sie für Amazon SES leasen, eine zusätzliche monatliche Gebühr. Bei der Nutzung von Dedicated IPs (Standard) gibt es keine Mindestverpflichtung.

Weitere Informationen zu den Kosten, die mit Dedicated IPs (Standard) verbunden sind, finden Sie unter Amazon SES Pricing.

Eine Liste aller Regionen, in denen Amazon SES derzeit verfügbar ist, finden Sie unter AWS-Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz. Weitere Informationen zur Anzahl der Availability Zones, die in jeder Zone verfügbar sind AWS-Region, finden Sie unter AWS Globale Infrastruktur.

Dedizierte IPs (Standard) anfragen oder aufgeben

Sie können so viele dedizierte IPs (Standard) anfordern, wie Sie benötigen, indem Sie im AWS Support Center einen Fall zur Erhöhung des Servicekontingents erstellen.

Um spezielle IPs Dienste (Standard) anzufordern oder aufzugeben

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Dedicated aus IPs.
3. Führen Sie eine der folgenden Aktionen aus:

   a. Wenn Sie IPs in Ihrem Konto noch keine Dedicated haben:

      - Die Dedizierte IPs Onboarding-Seite wird angezeigt. Wählen Sie im Übersichtsbereich Dedicated IPs (Standard) die Option Dedicated IPs Request aus.

   b. Wenn IPs in Ihrem Konto bereits dedizierte Dienste vorhanden sind:

      i. Wählen Sie auf der IPs Seite Dedicated die Registerkarte Standard-IP-Pools aus.

      ii. Wählen Sie im Bereich Standard Overview die Option Request oder Relinish Standard dedicated aus. IPs
4. Das Hallo! Wir sind hier, um die Hilfeseite in der AWS Support Console zu öffnen. Für alle Felder auf dieser Seite sind die folgenden Werte vorausgewählt:

   - Wählen Sie das entsprechende Thema für Ihren Fall aus — Konto und Abrechnung
   - Service — Service Quotas
   - Kategorie — Amazon SES
   - Schweregrad — Allgemeine Frage

   Nachdem Sie diese Werte überprüft haben, wählen Sie Nächster Schritt: Zusätzliche Informationen aus.
5. Füllen Sie unter Zusätzliche Informationen die folgenden Auswahlen aus:

   - Wählen Sie unter Region die Region aus, für AWS-Region die sich Ihre Anfrage bezieht.
   - Wählen Sie unter Kontingenttitel die Option Gewünschte dedizierte IP aus.
   - Wählen Sie unter Wert die Anzahl der dedizierten Geräte aus, die IPs Sie in der ausgewählten Region anfordern oder aufgeben möchten.
   - Wenn Sie Dedicated IPs (Standard) in einer anderen Region anfordern oder aufgeben möchten AWS-Region, wählen Sie Weiteres Limit hinzufügen und füllen Sie die Felder entsprechend aus. Wiederholen Sie den Vorgang für jedes weitere. AWS-Region

- Machen Sie unter Beschreibung deutlich, was Sie in jeder angegebenen Region haben und was Sie tun möchten, wie in den folgenden Beispielen dargestellt:

  Anfrage — „Ich habe zwei DIPs in der Region Mailand, möchte aber noch eine hinzufügen, also insgesamt drei“

  Geben Sie auf — „Ich habe zwei DIPs in der Region Ohio, möchte aber einen davon entfernen. Bitte entfernen Sie die DIP mit der Adresse 23.251.228.95“.

  > **Important**
  >
  > Der Prozess zur Freigabe einer dedizierten IP-Adresse kann nicht rückgängig gemacht werden. Wenn Sie eine dedizierte IP-Adresse in der Monatsmitte freigeben, berechnen wir die monatliche Nutzungsgebühr für die dedizierte IP anteilig auf Grundlage der im aktuellen Monat bereits verstrichenen Tage.

- Klicken Sie auf Next step: Solve now or contact us (()Nächster Schritt): Jetzt lösen oder Support kontaktieren).
- Wählen Sie auf der Seite „Jetzt lösen“ oder „Kontaktieren Sie uns“ Ihre bevorzugte Kontaktsprache aus und klicken Sie auf Senden.

Wir bearbeiten Ihren Antrag, nachdem Sie das Formular übermittelt haben. Wenn wir Ihrer Anfrage stattgeben, werden wir im Support Center auf Ihren Fall antworten, um zu bestätigen, dass die dedizierten IP-Adressen Ihrem Konto entsprechend Ihrer Anfrage hinzugefügt oder daraus entfernt wurden.

Aufwärmen dedizierter IP-Adressen (Standard)

Bei der Entscheidung, ob eine Nachricht akzeptiert oder abgelehnt wird, berücksichtigen die E-Mail-Dienstanbieter die Zuverlässigkeit der IP-Adresse, von der sie gesendet wurde. Einer der Faktoren, der zur Zuverlässigkeit einer IP-Adresse beiträgt, ist, ob die Adresse einen Verlauf an hochgradig erwünschten E-Mails aufweist. Es ist weniger wahrscheinlich, dass E-Mail-Anbieter Post von neuen IP-Adressen akzeptieren, die nur einen geringen oder gar keinen Verlauf aufweisen. E-Mails, die von IP-Adressen mit nur geringem oder ganz ohne Verlauf gesendet wurden, werden möglicherweise im Junk-Ordner des Empfängers abgelegt oder vollständig blockiert.

Wenn Sie damit beginnen, E-Mails von einer neuen dedizierten IP-Adresse aus zu versenden, sollten Sie die Menge der über diese Adresse versendeten E-Mails allmählich erhöhen, bevor Sie die Adresse mit voller Kapazität nutzen. Dieser Vorgang wird als Aufwärmen der IP-Adresse bezeichnet.

Die für das Aufwärmen einer IP-Adresse erforderliche Zeit ist je nach E-Mail-Anbieter unterschiedlich. Bei einigen E-Mail-Anbietern können Sie einen positiven Ruf in zwei Wochen erstellen, während es bei anderen bis zu sechs Wochen dauern kann. Beim Aufwärmen einer neuen dedizierten IP-Adresse sollten Sie E-Mails an Ihre aktivsten Benutzer senden, um sicherzustellen, dass Ihre Beschwerderate niedrig bleibt. Sie sollten auch Ihre Unzustellbarkeitsnachrichten sorgfältig durchsehen und weniger E-Mails senden, wenn Sie eine hohe Anzahl an Sperrungs- oder -Drosselungsbenachrichtigungen erhalten. Weitere Informationen zum Überwachen Ihrer Unzustellbarkeiten finden Sie unter Überwachen Ihrer Amazon SES-Sendeaktivität.

Automatisches Aufwärmen für spezielle Benutzer IPs (Standard)

Wenn Sie dedizierte IP-Adressen (Standard) anfordern, wärmt Amazon SES sie automatisch auf, um die Zustellungsrate der von Ihnen gesendeten E-Mails zu verbessern. Die automatische Aufwärmfunktion für IP-Adressen ist standardmäßig aktiviert. SES wärmt Ihr Gerät automatisch auf, IPs indem es die Anzahl der E-Mails, die Sie über Ihr Gerät versenden, auf der IPs Grundlage eines vordefinierten Aufwärmplans schrittweise erhöht. Diese schrittweise Erhöhung trägt dazu bei, dass Sie sich bei Internetdienstanbietern einen positiven Ruf IPs aufbauen ()ISPs.

Die Schritte, die während des automatischen Aufwärmprozesses durchgeführt werden, sind davon abhängig, ob Sie bereits über dedizierte IP-Adressen verfügen.

- Wenn Sie zum ersten Mal dedizierte IPs (Standard) anfragen, verteilt SES Ihren E-Mail-Versand auf Ihre dedizierten IP-Adressen und eine Reihe von Adressen, die mit anderen SES-Kunden geteilt werden. SES erhöht im Laufe der Zeit allmählich die Anzahl der Nachrichten, die über Ihre dedizierten IP-Adressen versendet werden.
- Wenn Sie bereits über dedizierte IP-Adressen verfügen, verteilt SES Ihren E-Mail-Versand zwischen Ihren bestehenden dedizierten IPs (die bereits vorgewärmt sind) und Ihren neuen dedizierten IPs (die nicht vorgewärmt sind). SES erhöht im Laufe der Zeit allmählich die Anzahl der Nachrichten, die über Ihre neuen dedizierten IP-Adressen versendet werden.

> **Note**
>
> Beim automatischen Aufwärmen von IPs handelt es sich um einen zeitbasierten Prozess. Der Anteil der aufgewärmten IPs steigt kontinuierlich über 45 Tage unabhängig von Ihrem Versandvolumen.

Nachdem Sie eine dedizierte IP-Adresse aufgewärmt haben, sollten Sie jeden Tag ca. 1.000 E-Mails an jeden E-Mail-Anbieter versenden, bei dem Sie einen positiven Ruf aufrechterhalten wollen. Führen Sie diese Aufgabe bei jeder dedizierten IP-Adresse durch, die Sie mit SES verwenden.

Versenden Sie keine großen E-Mail-Mengen unmittelbar nach dem Abschluss des Aufwärmprozesses. Erhöhen Sie stattdessen langsam die Anzahl der versendeten E-Mails, bis Sie Ihr Zielvolumen erreicht haben. Wenn ein E-Mail-Anbieter einen plötzlichen Anstieg der Anzahl von E-Mails feststellt, die über eine IP-Adresse versendet werden, wird er möglicherweise die Zustellung von Nachrichten über diese Adresse blockieren oder drosseln.

Deaktiviert den automatischen Aufwärmvorgang auf dedizierten Geräten (Standard) IPs

Beim Kauf neuer dedizierter Standard-IP-Adressen wärmt Amazon SES sie automatisch für Sie auf, da die automatische Aufwärmfunktion für IP-Adressen standardmäßig für Ihr Konto aktiviert ist. Wenn Sie es vorziehen, dedizierte IP-Adressen selbst aufzuwärmen, können Sie die automatische Aufwärmfunktion für alle Ihre IP-Adressen auf Kontoebene deaktivieren.

Wenn Sie die automatische Aufwärmfunktion deaktivieren, IPs werden alle später geleasten dedizierten Geräte Ihrem Konto mit dem Aufwärmstatus Abgeschlossen hinzugefügt, sodass sie auch ohne Warm-Up-Status verwendet werden können. Das bedeutet, dass Sie dafür verantwortlich sind, sicherzustellen, dass sie ordnungsgemäß aufgewärmt sind, bevor Sie sie für den regulären Versand verwenden. IPs Alle Geräte IPs , die sich zu dem Zeitpunkt, als Sie die automatische Aufwärmfunktion deaktiviert haben, gerade in der Warmlaufphase befanden, werden nicht aktiviert.

> **Important**
>
> Wenn Sie die automatische Aufwärmfunktion deaktivieren, sind Sie für das Aufwärmen Ihrer dedizierte IP-Adressen selbst verantwortlich. Wenn Sie E-Mails über Adressen versenden, die noch nicht aufgewärmt sind, kann dies schlechte Zustellungsraten zur Folge haben.

Um die automatische Aufwärmfunktion für alle dafür vorgesehenen (Standard-) Geräte in deinem Konto zu deaktivieren IPs (oder wieder zu aktivieren)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Dedicated aus IPs.
3. Wählen Sie auf der IPs Seite Dedicated die Registerkarte Standard-IP-Pools aus.
4. Wählen Sie im Bereich Standard overview (Standardübersicht) die Option Disable auto warm-up (Automatisches Aufwärmen deaktivieren) aus, wenn Sie das automatische Aufwärmen deaktivieren möchten, oder Enable auto warm-up (Automatisches Aufwärmen aktivieren), um es wieder zu aktivieren.

Dedizierte Geräte manuell IPs warmfahren (Standard)

Sie können Ihr zugewiesenes IPs (Standard-) aktuelles Sendelautstärke manuell erhöhen oder verringern, indem Sie den Aufwärmvorgang bearbeiten, den Aufwärmvorgang vorzeitig beenden, die aktuelle Sendelautstärke auf 0% setzen und den Aufwärmvorgang erneut starten.

Zum manuellen Aufwärmen von dedizierten Geräten (Standard) IPs

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Dedicated aus IPs.
3. Wählen Sie auf der IPs Seite Dedicated die Registerkarte Standard-IP-Pools aus.
4. Wählen Sie im dedizierten IPs Bereich „All Standard“ eine IP-Adresse aus, klicken Sie auf „Warm-up bearbeiten“ und wählen Sie eine der folgenden Optionen aus:

    a. Prozentsatz bearbeiten – Geben Sie einen Wert in das Feld Warm-up percentage (Aufwärmprozentsatz) ein, um das aktuelle Sendevolumen Ihrer IP zu erhöhen oder zu verringern, indem Sie den Aufwärmprozentsatz bearbeiten. Wählen Sie anschließend Save changes (Änderungen speichern) aus.

    In der Spalte Warm-up status (Aufwärmstatus) wird `In progress` und in der Spalte Warm-up percentage (Aufwärmprozentsatz) der von Ihnen eingegebene Wert angezeigt.

    b. Als abgeschlossen markieren – Sehen Sie sich das Dialogfenster Mark warm-up as Complete? (Aufwärmen als abgeschlossen markieren?) an, um zu bestätigen, dass Sie

die Auswirkungen einer vorzeitigen Beendigung des automatischen Aufwärmvorgangs verstehen. Wählen Sie dann Mark as Complete (Als abgeschlossen markieren) aus.

In der Spalte Warm-up status (Aufwärmstatus) wird `Complete` und in der Spalte Warm-up percentage (Aufwärmprozentsatz) `100%` angezeigt.

c. Prozentsatz zurücksetzen — lesen Sie den Prozentsatz für die Aufwärmphase zurücksetzen? Dialog zur Bestätigung, dass Sie die aktuelle Sendelautstärke der IP auf 1% einstellen und entweder den automatischen Aufwärmvorgang neu starten oder den Aufwärmprozentsatz manuell einstellen und dann Reset wählen müssen.

In der Spalte Warm-up status (Aufwärmstatus) wird `In progress` und in der Spalte Warm-up percentage (Aufwärmprozentsatz) `1%` angezeigt.

Erstellung von standardmäßigen dedizierten IP-Pools für dedizierte IPs (Standard)

Wenn Sie mehrere dedizierte IP-Adressen (Standard) für die Verwendung mit Amazon SES erworben haben, können Sie Gruppen dieser Adressen erstellen. Diese werden als dedizierte IP-Pools bezeichnet. Durch die Gruppierung von dedizierten IPs (Standard) in einem Pool sind sie einfacher zu verwalten. Ein häufiger Anwendungsfall besteht darin, einen Pool für den Versand von Marketingkommunikation und einen weiteren für den Versand von Transaktions-E-Mails zu erstellen. Ihre Absender-Reputation für transaktionale E-Mails wird dann von der für Ihre Marketing-E-Mails getrennt. In diesem Szenario wird die Zustellung Ihrer transaktionalen E-Mails nicht beeinträchtigt, wenn eine Marketingkampagne eine große Anzahl von Beschwerden hervorruft.

Dieser Abschnitt enthält Verfahren zum Erstellen von dedizierten IP-Pools.

> **Note**
>
> Sie können auch Konfigurationssätze erstellen, die einen Pool von IP-Adressen verwenden, welche von allen SES-Kunden gemeinsam genutzt werden. Der gemeinsam genutzte IP-Pool ist nützlich in Situationen, in denen Sie E-Mails versenden müssen, die nicht mit Ihrem gewohnten Sendeverhalten übereinstimmen. Informationen zur Verwendung des gemeinsam genutzten IP-Pools mit einem Konfigurationssatz finden Sie unter Zuweisen von IP-Pools in Amazon SES.

Um mithilfe der SES-Konsole einen dedizierten IP-Pool für dedizierte IPs (Standard) zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Dedicated aus IPs.

   > **Note**
   >
   > Wenn Sie derzeit keine dedizierten Produkte IPs (Standard) in Ihrem Konto haben, wird die Seite Dedicated IPs Onboarding angezeigt, auf der Sie die Möglichkeit haben, Dedicated IPs (Standard) zu erwerben. Weitere Informationen finden Sie unter the section called “Dedizierte IPs (Standard) anfragen oder aufgeben”.

3. Wählen Sie auf der IPs Seite Dediziert die Registerkarte Standard-IP-Pools aus.
4. Wählen Sie im Bereich All Dedicated IP (standard) pools (Alle dedizierten Standard-IP-Pools) die Option Create Standard IP pool (Standard-IP-Pool erstellen) aus.

   Die Seite Create IP Pool (IP-Pool erstellen) wird geöffnet.
5. Im Bereich Pool details (Pool-Details):

   a. Wählen Sie im Feld Scaling mode (Skalierungsmodus) die Option Standard (self managed) (Standard (selbstverwaltet)) aus.

   b. Geben Sie im Feld IP pool name (IP-Pool-Name) einen Namen für Ihren IP-Pool ein.

      > **Note**
      >
      > Der IP-Pool-Name muss eindeutig sein und darf kein Duplikat eines verwalteten IP-Pool-Namens in Ihrem Konto sein.

   c. (Optional) Wenn Sie bereits dedizierte Standard-IP-Adressen haben, die Sie diesem IP-Pool hinzufügen möchten, wählen Sie diese aus der Dropdown-Liste im Feld Dedicated IP addresses (Dedizierte IP-Adressen) aus.

      > **Note**
      >
      > Wenn Sie eine IP-Adresse auswählen, die bereits einem IP-Pool zugeordnet ist, wird sie jetzt nur noch mit diesem IP-Pool verknüpft.

6. (Optional) Sie können diesen IP-Pool einem Konfigurationssatz zuordnen, indem Sie einen Satz aus der Dropdown-Liste im Feld Configuration sets (Konfigurationssätze) auswählen.

   > **Note**
   >
   > - Wenn Sie einen Konfigurationssatz auswählen, der bereits einem IP-Pool zugeordnet ist, wird er jetzt nur noch mit diesem IP-Pool verknüpft.
   > - Wenn Sie verknüpfte Konfigurationssätze hinzufügen oder entfernen möchten, nachdem dieser IP-Pool erstellt wurde, bearbeiten Sie den Parameter Sending IP pool (Senden des IP-Pools) des Konfigurationssatzes.
   > - Wenn Sie noch keine Konfigurationssätze erstellt haben, lesen Sie Konfigurationssätze.

7. (Optional) Sie können diesem IP-Pool ein oder mehrere Tags hinzufügen, indem Sie einen Tag-Schlüssel und einen optionalen Wert für den Schlüssel einschließen.

   a. Klicken Sie aufNeues Tag hinzufügenund geben Sie den WertSchlüsselaus. Sie können einen optionalen Wert für das Tag unter Value (Wert) hinzufügen.

   b. Wählen Sie zum Speichern der Änderungen Add Bot User aus.

   Sie können bis zu 50 Tags hinzufügen. Sie können jede vorhandene Zeile entfernen, indem Sie Tag entfernen auswählen.

8. Wählen Sie Create pool (Pool erstellen) aus.

   > **Note**
   >
   > Nachdem Sie einen Standard-IP-Pool erstellt haben, kann dieser in einen verwalteten IP-Pool konvertiert werden. Siehe Erstellen eines verwalteten IP-Pools.

Dedizierte IP-Adressen (verwaltet) für Amazon SES

Dedizierte IP-Adressen (verwaltet) ist eine Amazon-SES-Funktion, die dedizierte IP-Adressen in Ihrem Namen automatisch einrichtet und verwaltet, um eine schnelle und einfache Möglichkeit zu bieten, dedizierte IP-Adressen zu verwenden, die von SES verwaltet werden. Auf diese Weise können Sie sicherstellen, dass Ihre dedizierten IP-Adressen effizient und optimal für den E-Mail-Versand verwendet werden.

Um Dedicated IPs (Managed) in Ihrem Konto zu aktivieren, erstellen Sie einfach einen verwalteten IP-Pool und SES erledigt den Rest. SES bestimmt anhand Ihrer Sendemuster, wie viele dedizierte Geräte IPs Sie benötigen, erstellt sie für Sie und verwaltet dann, wie sie auf der Grundlage Ihrer Sendeanforderungen skaliert werden.

Nach der Aktivierung können Sie dediziert IPs (verwaltet) für Ihren E-Mail-Versand verwenden, indem Sie den verwalteten IP-Pool einem Konfigurationssatz zuordnen und diesen Konfigurationssatz dann beim Senden von E-Mails angeben. Der Konfigurationssatz kann auch auf eine sendende Identität angewendet werden, indem ein Standardkonfigurationssatz verwendet wird.

Vorteile und Funktionen von Dedicated IPs (Managed)

Die dedizierten IP-Adressen, die Sie mit dedizierten IPs (verwalteten) IP-Adressen erstellen, automatisieren Verwaltungsaufgaben und tragen so dazu bei, dass Ihre dedizierten IP-Adressen optimal für den E-Mail-Versand verwendet werden:

- Einfaches Onboarding — Um mit Dedicated IPs (Managed) loszulegen, erstellen Sie direkt von der SES-Konsole aus einen verwalteten IP-Pool. Dedizierte IP-Adressen werden dem Pool automatisch zugewiesen. Sie können mit dem Senden mit dem verwalteten IP-Pool beginnen, ohne einen Anforderungsfall über das AWS Support Center öffnen zu müssen.
- Automatische Skalierung pro ISP — Sie müssen Ihre dedizierten IP-Pools nicht manuell überwachen oder skalieren, da der verwaltete IP-Pool je nach Nutzung automatisch skaliert wird. Er berücksichtigt auch ISP-spezifische Richtlinien. Wenn SES beispielsweise feststellt, dass ein ISP ein niedriges tägliches Sendekontingent unterstützt, wird der Pool aufskaliert, um den Datenverkehr an diesen ISP besser auf mehr IP-Adressen zu verteilen.
- Intelligentes Warmup — Dedizierter IPs (verwalteter) Start, an den E-Mails ISPs je nach Kapazität gesendet werden. Dabei wird berücksichtigt, wie stark sie derzeit aufgewärmt sind. Sie verfolgen automatisch den Aufwärmgrad für jeden ISP einzeln. Darüber hinaus bietet die spezielle IPs (verwaltete) Funktion Informationen über Ihren Ruf zu einem effektiven Tagespreis mit Top-Tarifen ISPs in Form von CloudWatch Amazon-Metriken und integrierten Dashboards.
  - Aufwärmen pro ISP – SES verfolgt die Reputation für jede IP im verwalteten IP-Pool für jeden ISP einzeln. Wenn Sie beispielsweise Ihren gesamten Datenverkehr an Gmail gesendet haben, gelten die IP-Adressen nur für Gmail als aufgewärmt und für andere als kalt. ISPs Wenn Sie Ihr Datenverkehrsmuster ändern, indem Sie an Hotmail gesendete E-Mails hochfahren, erhöht SES den Datenverkehr für Hotmail langsam, da die IP-Adressen noch nicht aufgewärmt sind.
  - Adaptives Aufwärmen und Umstellung auf gemeinsam genutzte Pools — Die Anpassung der Aufwärmphase ist adaptiv und berücksichtigt die tatsächlichen Sendemuster. Wenn das

Sendevolumen an einen ISP sinkt, verringert sich auch der Aufwärmprozentsatz für diesen ISP. In der frühen Phase des Aufwärmens werden alle Sendungen, die aufgrund des aktuellen Aufwärmstatus übermäßig sind, über die IP-Adressen gesendet, die mit anderen Amazon SES SES-Benutzern gemeinsam genutzt werden — den gemeinsam genutzten SES-Pool. In späteren Aufwärmphasen werden übermäßige Sendeaktivitäten proaktiv verlangsamt und später erneut versucht.

> **Important**
>
> Dediziert IPs (verwaltet) wärmt Ihre dedizierten IP-Adressen zwar automatisch auf, ein Teil dieses automatischen Prozesses arbeitet jedoch interaktiv mit dem gemeinsam genutzten SES-IP-Pool zusammen.
>
> - Wenn Ihre Senderate für Ihre neuen dedizierten Geräte zu hoch ist, IPs während sie aufgewärmt werden, überträgt SES automatisch einen Teil Ihres Sendens in den gemeinsam genutzten SES-IP-Pool, um den Ruf Ihrer neuen dedizierten IP-Adresse zu schützen. IPs
> - Selbst wenn Ihre neuen Dedicated vollständig aufgewärmt IPs sind, kann nicht garantiert werden, dass Ihre gesamten Sendungen sie zu 100% durchlaufen. Wenn Ihre Senderate beispielsweise plötzlich ansteigt und Dedicated IPs (Managed) feststellt, dass eine zusätzliche dedizierte IP-Adresse zugewiesen werden muss, wird der Aufwärmvorgang eingeleitet, der die Nutzung des gemeinsamen Pools beinhaltet. Wenn Ihre Senderate plötzlich sehr niedrig ist, könnte Ihr gesamtes Senden ebenfalls auf den gemeinsam genutzten SES-IP-Pool umgestellt werden, siehe. the section called “Bedeutung des Aufwärmens”

- Automatische Anforderung und Weitergabe von dedizierten IP-Adressen — Sie müssen verwaltete dedizierte IP-Adressen nicht über das AWS Support Center anfordern oder aufgeben, wie dies bei der Verwendung von dedizierten IP-Adressen (Standard) erforderlich ist. IPs Beim Onboarding mit dedizierten IPs (verwalteten) Verbindungen direkt über die SES-Konsole, CLI oder API werden Ihnen automatisch dedizierte IP-Adressen zugewiesen, und es wird eine Gebühr berechnet, die auf dem Volumen der von Ihnen gesendeten Nachrichten basiert. Wenn Sie einen IP-Pool löschen, der durch Dedicated IPs (Managed) oder Dedicated IPs (Managed) erstellt wurde, werden Ihre zugewiesenen IP-Adressen automatisch gelöscht und die Gebühren fallen sofort weg.
  - Ermitteln Ihrer ersten dedizierten IP-Adresse — Die dedizierte IPs (verwaltete) Funktion weist Ihnen automatisch Ihre erste dedizierte IP-Adresse zu, sobald Ihr Versandvolumen innerhalb weniger Tage Hunderte von E-Mails erreicht. Dadurch wird sichergestellt, dass die IP-Adresse,

von der aus Sie senden, eine Reputation als Absender aufbauen und die Zustellbarkeit verbessern kann. (Wenn Sie nicht davon ausgehen, dass Ihr Sendevolumen diesen Umfang erreichen wird, sollten Sie gemeinsam genutzte IP-Adressen verwenden. In der Vergleichstabelle unter Dedizierte IP-Adressen finden Sie Informationen darüber, welche Arten von IP-Adressen sich jeweils am besten für den Versand von E-Mails eignen.)

Darum ist das richtige Aufwärmen von IP-Adressen entscheidend

Um sicherzustellen, dass Ihre E-Mail über Ihre dedizierte IP-Adresse zugestellt wird, muss sie beim empfangenden ISP einen guten Ruf haben. ISPs akzeptiert nur eine geringe Menge an E-Mails von einer IP-Adresse, die sie nicht erkennen. Wenn Ihnen eine IP erstmalig zugewiesen wird, ist diese neu und wird vom empfangenden ISP nicht erkannt, da noch keine Reputation mit ihr verbunden ist. IP-Adressen müssen langsam Vertrauen bei den empfangen ISP aufbauen, damit sich auch ihre Reputation festigen kann. Dieser schrittweise Vertrauensaufbau wird als Aufwärmen bezeichnet. Unmittelbar nach der dedizierten IPs (verwalteten) Zuweisung einer IP wird der intelligente Aufwärmvorgang gestartet.

Mit den Funktionen „Aufwärmen pro ISP“ und „Adaptives Aufwärmen“ von Dedicated IPs (Managed) wird die Geschäftskontinuität während des gesamten Aufwärmzyklus gewährleistet, indem sichergestellt wird, dass Ihre E-Mails zugestellt werden. Sobald die Aufwärmphase abgeschlossen ist, wird jegliche überschüssige Kapazität in die Warteschlange gestellt und nur über den dedizierten IP-Pool gesendet. Wenn Sie jedoch über eine dedizierte IP-Adresse verfügen und Ihr Versand unter das Mindestvolumen fällt, das zur Aufrechterhaltung der IP-Reputation erforderlich ist, kann Dedicated IPs (Managed) Ihre dedizierte IP-Adresse entfernen und Ihr Versand wird über den gemeinsam genutzten SES-IP-Pool geleitet.

> **Note**
>
> Wenn Sie kleinere E-Mail-Volumen (weniger als einige Hundert pro Tag innerhalb von wenigen Tagen) senden, wäre es vorteilhafter, sie über den gemeinsam genutzten IP-Pool von SES zu senden. Finden Sie anhand der Vergleichstabelle unter heraus, ob die dedizierte IPs (verwaltete) Methode für den E-Mail-Versand geeignet ist. Dedizierte IP-Adressen

Verstehen Sie die gemeinsame Verantwortung zwischen Ihnen und SES bei der Nutzung von dedicated IPs (verwaltet)

Dedizierte IP-Adressen (verwaltet) bieten zwar zahlreiche automatisierte Funktionen für dediziertes IP-Management, Skalierung und Warmup, doch müssen der Umfang dieser Automatisierung und die Aufgaben von SES geklärt werden. Es wäre falsch anzunehmen, dass „verwaltet“ bedeutet, dass SES sich vollständig um alle Aspekte der IP-Reputation und der Listung kümmert. Um diese Missverständnisse auszuräumen, müssen wir betonen, dass der Service zwar technische Aspekte wie Skalierung und Aufwärmphase automatisiert, Sie aber weiterhin dafür verantwortlich sind, Ihre Senderreputation aufrechtzuerhalten und alle Probleme im Zusammenhang mit der Reputation zu lösen, z. B. die Aufnahme in eine Reputation Block List (RBL).

Im Folgenden wird das FAQs Modell der gemeinsamen Verantwortung zwischen Ihnen und SES erläutert und häufig vorkommende Missverständnisse über den Umfang des Services ausgeräumt. In diesen häufig gestellten Fragen wird darauf hingewiesen, dass sich der Aspekt „gemanagt“ zwar auf die Verwaltung der technischen Infrastruktur bezieht, Sie jedoch Ihren Ruf als Absender aktiv überwachen und pflegen, die Absprungraten niedrig halten und die meisten Anfragen zur Streichung von RBLs von der Liste selbst bearbeiten müssen:

- the section called “Verwaltetes DIPS FAQs”

Erstellen eines verwalteten IP-Pools zur Aktivierung eines dedizierten (verwalteten) IPs

Um dediziert IPs (verwaltet) zu aktivieren, erstellen Sie zunächst einen verwalteten IP-Pool. Nachdem Sie einen verwalteten Pool erstellt haben, bestimmt die Funktion anhand Ihrer Sendemuster, wie viele dedizierte Pools IPs Sie benötigen, und skaliert sie dynamisch an Ihre Anforderungen.

Wenn Sie Ihren verwalteten Pool zum Senden von E-Mails verwenden möchten, müssen Sie den verwalteten Pool mit einem Konfigurationssatz verknüpfen und diesen Konfigurationssatz dann beim Senden von E-Mails angeben. Der Konfigurationssatz kann auch auf eine sendende Identität angewendet werden, indem ein Standardkonfigurationssatz verwendet wird.

Es gibt zwei Möglichkeiten, einen verwalteten IP-Pool zu erstellen:

- Einen neuen Pool erstellen
- Einen vorhandenen Pool von einem Standard- in einen verwalteten Pool umwandeln

Im Folgenden werden Anleitungen für beide Methoden bereitgestellt.

Mithilfe der SES-Konsole einen verwalteten IP-Pool erstellen oder einen Standard- in einen verwalteten Pool umwandeln

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Dedicated aus IPs.
3. Befolgen Sie je nachdem, ob Sie einen neuen verwalteten IP-Pool erstellen oder einen dedizierten Standard-IP-Pool in einen verwalteten Pool umwandeln möchten, die entsprechenden Anweisungen:

   Create new pool

   Einen neuen verwalteten IP-Pool erstellen

   1. Führen Sie eine der folgenden Aktionen aus:

      a. Wenn Sie IPs in Ihrem Konto noch keine Dedicated haben:

         - Die Dedizierte IPs Onboarding-Seite wird angezeigt. Wählen Sie im Übersichtsbereich Dedicated IPs (managed) die Option Dedicated IPs aktivieren aus.

           Die Seite Create IP Pool (IP-Pool erstellen) wird geöffnet.

      b. Wenn Sie IPs in Ihrem Konto bereits Dedicated haben:

         i. Wählen Sie auf der IPs Seite Dediziert die Registerkarte Verwaltete IP-Pools aus.

         ii. Wählen Sie im Bereich All Dedicated IP (standard) pools (Alle dedizierten IP-Pools (Standard)) die Option Create Managed IP pool (Verwalteten IP-Pool erstellen) aus.

           Die Seite Create IP Pool (IP-Pool erstellen) wird geöffnet.

   2. Im Bereich Pool details (Pool-Details):

      a. Wählen Sie im Feld Scaling mode (Skalierungsmodus) die Option Managed (auto managed) (Verwaltet (automatisch verwaltet)) aus.

b. Geben Sie im Feld IP pool name (IP-Pool-Name) einen Namen für Ihren verwalteten Pool ein.

> **Note**
>
> - Der IP-Pool-Name muss eindeutig sein. Es darf kein Duplikat eines dedizierten Standard-IP-Pool-Namens in Ihrem Konto sein.
> - Ihr Konto kann maximal 50 dedizierte IP-Pools pro AWS-Region aufweisen, einschließlich verwalteter und Standard-IP-Pools.

3. (Optional) Sie können diesen verwalteten IP-Pool einem Konfigurationssatz zuordnen, indem Sie einen Satz aus der Dropdown-Liste im Feld Configuration sets (Konfigurationssätze) auswählen.

> **Note**
>
> - Wenn Sie einen Konfigurationssatz auswählen, der bereits einem IP-Pool zugeordnet ist, wird er mit diesem verwalteten Pool verknüpft und ist nicht mehr dem vorherigen Pool zugeordnet.
> - Wenn Sie verknüpfte Konfigurationssätze hinzufügen oder entfernen möchten, nachdem dieser verwaltete Pool erstellt wurde, bearbeiten Sie den Parameter Sending IP pool (Senden des IP-Pools) des Konfigurationssatzes im Bereich General details (Allgemeine Details).
> - Wenn Sie noch keine Konfigurationssätze erstellt haben, lesen Sie Konfigurationssätze.

4. (Optional) Sie können Ihrem IP-Pool mindestens einen Tag hinzufügen, indem Sie einen Tag-Schlüssel und einen optionalen Wert für den Schlüssel einbeziehen.

   a. Klicken Sie aufNeues Tag hinzufügenund geben Sie den WertSchlüsselaus. Sie können einen optionalen Wert für das Tag unter Value (Wert) hinzufügen. Sie können bis zu 50 Tags hinzufügen. Wenn Sie einen Fehler machen, wählen Sie Remove (Entfernen) aus.

   b. Wählen Sie zum Hinzufügen der Tags Save changes (Änderungen speichern) aus.

Nachdem Sie den Pool erstellt haben, können Sie einen Tags hinzufügen, entfernen oder bearbeiten, indem Sie den verwalteten Pool und Edit (Bearbeiten) auswählen.

5. Wählen Sie Create pool (Pool erstellen) aus.

> **Note**
>
> - Nachdem Sie einen verwalteten IP-Pool erstellt haben, kann dieser nicht in einen Standard-IP-Pool konvertiert werden.
> - Wenn Sie Dedicated IPs (Managed) verwenden, können Sie pro AWS-Region Konto nicht mehr als 10.000 Sende-Identitäten (Domains und E-Mail-Adressen, in beliebiger Kombination) haben.

Convert standard to managed

Einen dedizierten Standard-IP-Pool in einen verwalteten Pool umwandeln

1. Wählen Sie auf der IPs Seite Dediziert die Registerkarte Standard-IP-Pools aus.
2. Markieren Sie im Bereich Alle dedizierten IP-Pools (Standard) das Kontrollkästchen des dedizierten IP-Pools, den Sie vom Standard- in einen verwalteten Pool umwandeln möchten.
3. Wählen Sie In verwalteten Pool umwandeln. Lesen Sie das Dialogfeld In verwalteten IP-Pool umwandeln, um sicherzustellen, dass Sie die Bedingungen für die Umwandlung des dedizierten Standard-IP-Pools in einen verwalteten Pool verstehen.

> **Note**
>
> Beachten Sie Folgendes, bevor Sie den dedizierten IP-Pool vom Standard- in einen verwalteten Pool umwandeln:
>
> 1. Alle Ihre aktuellen dedizierten IPs (Standard-) Daten werden in den verwalteten Pool verschoben.
> 2. Wenn Sie derzeit zu viele Dedicated IPs (Standard) für Ihr Sendevolumen leasen, entfernt Dedicated IPs (Managed) die überflüssigen IPs.
> 3. Wenn einige Ihrer dedizierten IPs (Standard-) Anwendungen Teil einer Zulassungsliste für andere Anwendungen sind, sollten Sie sie nicht in den

verwalteten Pool übertragen, da sie entfernt werden, wenn sie überflüssig werden — siehe Punkt 2.

4. Es fallen keine Gebühren mehr pro IP-Adresse an. Die Gebühren hängen jetzt vom Volumen ab, das Sie über den verwalteten Pool senden. Siehe Amazon SES – Preise.

4. Wenn Sie den angegebenen Bedingungen zustimmen, klicken Sie auf Bestätigen. Daraufhin wird ein Banner mit der Bestätigung angezeigt, dass Ihr dedizierter Standard-IP-Pool in einen verwalteten Pool umgewandelt wurde.

> **Note**
>
> Alle Konfigurationssätze oder Tags, die vor der Umwandlung dem Standard-Pool zugeordnet waren, werden nun dem verwalteten Pool zugeordnet. Dadurch ist ein nahtloser Übergang für jeden E-Mail-Versand gewährleistet, der den Konfigurationssatz verwendet.

Sie können die Ereignisveröffentlichung verwenden, um die Sendeleistung des verwalteten Pools nachzuverfolgen. Weitere Informationen finden Sie unter the section called “Überwachen des E-Mail-Versands mithilfe der Ereignisveröffentlichung”.

Anzeigen von Versand und Kapazität des verwalteten IP-Pools in der Amazon-SES-Konsole

Für die von Ihnen erstellten verwalteten IP-Pools bietet die SES-Konsole eine einfache Möglichkeit, anhand von Karten und Zeitreihendiagrammen mit Sendemetriken sowie Informationen zu ISP-Auslastung und -Kapazität zu überwachen, wie sie für Ihren E-Mail-Versand verwendet werden.

Versand und Kapazität des verwalteten IP-Pools in der Amazon-SES-Konsole anzeigen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Dedicated aus IPs.
3. Wählen Sie auf der IPs Seite Dedicated die Registerkarte Managed IP Pools aus.
4. Je nachdem, ob Sie Versand- und Kapazitätsmetriken in der Amazon SES SES-Konsole oder der CloudWatch Amazon-Konsole anzeigen möchten, folgen Sie den jeweiligen Anweisungen:

Amazon SES console

Versand- und Kapazitätsmetriken in der Amazon-SES-Konsole anzeigen

1. Wählen Sie in der Tabelle Alle dedizierten IP-Pools (verwaltet) den Namen eines verwalteten IP-Pools in der Spalte IP-Pool aus, um die zugehörigen Details anzuzeigen.

   Die Detailseite des ausgewählten IP-Pools wird mit den folgenden Karten und Zeitreihendiagrammen geöffnet:

   a. Karten:

      - Versandstatus — Zeigt an, ob Ihr Versandvolumen und Ihre Sendefrequenz ausreichen, um Dedicated zu nutzen, IPs indem einer von zwei Status angezeigt wird:
        - Unzureichendes Volumen – das Sendevolumen ist zu gering.
        - Senden über Dedicated IPs — In Ihrem verwalteten Pool IPs werden ein oder mehrere Dedicated verwendet.
      - Verwaltetes dediziertes IP-Sendevolumen — Das Volumen der E-Mails, die IPs in den letzten 7 Tagen über einen dedizierten Server in Ihrem verwalteten Pool gesendet wurden.
      - Prozentsatz der verwalteten dedizierten IP-Sendungen — Der Prozentsatz der E-Mails, die IPs in den letzten 7 Tagen über dedizierte E-Mails in Ihrem verwalteten Pool gesendet wurden.

   b. Diagramme:

      - Volumen der gesendeten E-Mails — Das Volumen der E-Mails, die in den letzten 7 Tagen über Managed Dedicated IPs versendet wurden, im Vergleich zu gemeinsam genutzten E-Mails IPs.
      - Prozentsatz des gesendeten Volumens — Der Prozentsatz der E-Mails, die in den letzten 7 Tagen über Managed Dedicated IPs versendet wurden, im Vergleich zu geteilten E-Mails IPs.
      - ISP-Kapazität — Zeigt an, wie viele E-Mails IPs in Ihrem verwalteten Pool über die 10 am häufigsten genutzten E-Mails gesendet wurden ISPs und welche Kapazität während des Versands verfügbar ist:

- Sendungen über ISP (rote Balken) – das E-Mail-Volumen, das Sie in den letzten 24 Stunden über den ausgewählten ISP gesendet haben.
- Kapazität des ISP (blauer Balken) – die verfügbare Kapazität des ausgewählten ISP in den letzten 24 Stunden.

2. Um das Diagramm zur ISP-Kapazität nach einem bestimmten ISP zu filtern, wählen Sie das ISP-Listenfeld und anschließend einen ISP aus. Das Diagramm wird mit den Metriken zum ausgewählten ISP aktualisiert. (Wenn Sie nicht nach einem ISP filtern, wird standardmäßig Gmail angezeigt.)

Amazon CloudWatch console

So zeigen Sie Versand- und Kapazitätsmetriken in der CloudWatch Amazon-Konsole an

- Wählen Sie in der Tabelle All Dedicated IP (Managed) Pools in der Metrikspalte den Link CloudWatch CloudWatchMetriken anzeigen aus, um die zugehörigen Details anzuzeigen. <pool_name>

  Die Seite des ausgewählten IP-Pools wird in der CloudWatch Konsole geöffnet und zeigt die folgenden Metriken an:

  - Senden — Die Menge der E-Mails, die sowohl über verwaltete, dedizierte IPs als auch gemeinsam genutzte E-Mails gesendet wurden IPs.
  - ApproximateDedicatedSendingPercentage— Gibt den ungefähren Prozentsatz des Datenverkehrs an, der über eine dedizierte IP zugestellt wurde.
  - SentLast24 Stunden — Die Menge an E-Mails, die Sie in den letzten 24 Stunden über den ausgewählten ISP gesendet haben. (In der SES-Konsole mit Sendungen über ISP bezeichnet.)
  - Available24 HourSend — Die verfügbare Kapazität des ausgewählten ISP in den letzten 24 Stunden. (In der SES-Konsole mit Kapazität des ISP bezeichnet.)

Löschen eines verwalteten IP-Pools und Abmeldung vom dedizierten IPs (verwalteten)

Wenn Sie einen verwalteten IP-Pool löschen, werden alle ihm zugewiesenen IP-Adressen automatisch aufgegeben. Wenn Sie nur einen verwalteten IP-Pool haben und diesen löschen, oder

wenn Sie Ihren letzten verbleibenden verwalteten IP-Pool löschen, deaktivieren Sie die dedizierte IPs (verwaltete) Funktion und die Gebühren fallen sofort weg.

So löschen Sie einen verwalteten IP-Pool mit der SES-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Dedicated aus IPs.
3. Wählen Sie auf der IPs Seite Dedicated die Registerkarte Managed IP Pools aus.
4. Wählen Sie in der Tabelle All Dedicated IP (managed) pools (Alle Pools mit dedizierten IPs (verwaltet)) das Optionsfeld neben dem Namen vom IP pool (IP-Pool) des verwalteten Pools aus, den Sie entfernen möchten, und wählen Sie Delete (Löschen) aus.
5. Im Popup-Modal können Sie Ihre Auswahl bestätigen, indem Sie Delete (Löschen) oder Cancel (Abbrechen) auswählen, um Ihren verwalteten Pool zu behalten.

> **Note**
>
> Wenn Sie nur einen verwalteten Pool haben oder Ihren letzten verwalteten Pool entfernen, werden Sie im Popup-Fenster daran erinnert, dass Sie durch das Löschen Ihres verbleibenden verwalteten Pools die dedizierte IPs (verwaltete) Funktion deaktivieren und dass Ihnen dafür keine Gebühren mehr berechnet werden. Sie müssen `Disable` in das Bestätigungsfeld eingeben, bevor Sie Delete (Löschen) auswählen können.

Verwenden Ihrer eigenen IP-Adressen zum Senden von E-Mails mit Amazon SES

Amazon SES enthält eine Funktion namens Bring Your Own IP (BYOIP), die es ermöglicht, Ihre eigenen IP-Adressen zum Senden von E-Mails zu verwenden . Wenn Sie bereits eine Reihe von IP-Adressen zum Senden von E-Mails verwenden, können Sie beantragen, dass wir Ihren IP-Bereich für den Versand von E-Mails per Amazon SES zur Verfügung stellen.

> **Note**
>
> BYOIP ist nur für dedizierte IP-Adressen verfügbar, die Sie manuell konfigurieren — es kann nicht mit Dedicated (verwaltet) verwendet werden. IPs

BYOIP ist zum Beispiel hilfreich, wenn Sie eine positive IP-Zuverlässigkeit mit einem internen E-Mail-Sende-System entwickelt haben, aber zu Amazon SES migrieren möchten. Durch die Verwendung von BYOIP können Sie sofort E-Mails per Amazon SES versenden, ohne die Zuverlässigkeiten Ihrer IP-Adressen wiederherstellen zu müssen.

Voraussetzungen

Um BYOIP nutzen zu können, muss Ihr IP-Adressbereich folgende Anforderungen erfüllen:

- Der Adressbereich muss bei Ihrer regionalen Internet Registry (RIR) registriert sein (z. B. American Registry for Internet Numbers (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE) oder Asia-Pacific Network Information Centre (APNIC)). Der Adressbereich muss für ein Unternehmen oder eine Organisation registriert sein und nicht für eine Einzelperson.
- Sie müssen den Nachweis erbringen können, dass Sie den Adressbereich besitzen, indem Sie eine signierte Autorisierungsnachricht übermitteln.
- Die Adressen im IP-Adressbereich müssen über einen sauberen Verlauf verfügen. Wir könnten die Zuverlässigkeit des IP-Adressbereichs untersuchen und uns das Recht vorbehalten, einen IP-Adressbereich abzulehnen, wenn er eine IP-Adresse enthält, die eine schlechte Zuverlässigkeit hat oder mit schädlichem Verhalten in Verbindung gebracht wird.
- Der IP-Adressbereich darf keine IP-Adressbereiche enthalten, die AWS-Service für BYOIP in einen anderen übertragen wurden, z. B. Amazon EC2.

Überlegungen

Es gibt mehrere Faktoren, die Sie berücksichtigen sollten, bevor Sie die Übertragung Ihrer IP-Bereiche auf Amazon SES anfordern:

- Der spezifischste Adressbereich, den Sie angeben können, ist /24. Mit anderen Worten, wenn Sie den IP-Bereich 203.0.113.0/24 auf Ihr Amazon SES-Konto übertragen, können Sie von insgesamt 256 Adressen senden, die von 203.0.113.0 bis 203.0.113.255 reichen. Sie müssen den

gesamten Bereich übertragen — Amazon SES erlaubt Ihnen derzeit nicht, einzelne IP-Adressen zu übertragen.

- Wenn Sie BYOIP für einen bestimmten Bereich von IP-Adressen verwenden, können Sie nur über eine einzelne AWS-Region auf diesen Bereich zugreifen.
- Sie können fünf Adressbereiche pro Region in Ihr AWS-Konto-Konto aufnehmen.
- Wenn Sie Ihre eigenen IP-Adressen verwenden, können Sie die Adressen im Pool der freigegebenen Amazon SES-IP-Adressen nicht verwenden. Wenn Sie diese gemeinsam genutzten IP-Adressen verwenden müssen, können Sie Amazon SES in einer anderen AWS-Region verwenden oder eine neue erstellen AWS-Konto.
- Für jede IP-Adresse, die Sie mit BYOIP verwenden, fällt eine monatliche Gebühr an. Weitere Informationen finden Sie unter Amazon SES – Preise.

Eigene IP-Adressen mit Amazon SES verwenden

Da wir verhindern möchten, dass unerwünschte oder schädliche Inhalte in unseren Systemen eingehen, müssen wir jede BYOIP-Anfrage sorgfältig prüfen.

Wenn Sie Ihren eigenen IP-Bereich mit Amazon SES verwenden möchten, senden Sie die folgenden Informationen an ses-byoip-request@amazon .com:

- Ihre AWS Konto-ID.
- Der AWS-Region , in dem Sie den IP-Bereich verwenden möchten, z. B. ap-south-1.
- Eine Beschreibung Ihres Anwendungsfalls
- Der IP-Bereich, den Sie mit Amazon SES nutzen möchten.
- Der Name der Internetregistrierung, mit der der Bereich registriert ist.

Wir werden an Geschäftstagen binnen 48 Stunden auf Ihren Antrag antworten. In unserer Kommunikation mit Ihnen werden wir möglicherweise zusätzliche Informationen anfordern, einschließlich Dokumente, die Ihre Eigentumsrechte an dem IP-Bereich belegen.

Virtueller Zustellbarkeitsmanager für Amazon SES

Die Zustellbarkeit oder die Sicherstellung, dass Ihre E-Mails die Posteingänge der Empfänger und nicht Spam- oder Junk-Ordner erreichen, ist ein Kernelement einer erfolgreichen E-Mail-Strategie.

Der virtuelle Zustellbarkeitsmanager ist eine Amazon-SES-Funktion, mit der Sie die E-Mail-Zustellbarkeit steigern können, z. B. die Verbesserung der Posteingangszustellung und der E-Mail-Konversionen, indem sie Einblicke in Ihre Sende- und Zustellungsdaten bietet und Ratschläge gibt, wie Sie Probleme beheben können, die sich negativ auf Ihre Erfolgsquote und die Reputation bei der Zustellung auswirken.

Warum die Posteingangszustellbarkeit und die Reputation Ihres Absenders wichtig sind

Die Posteingangszustellbarkeit ist ein Schlüsselfaktor, wenn es um E-Mail-Konversionen geht (wenn ein Empfänger nach dem Öffnen einer E-Mail eine Aktion ergreift) – Kunden, die Ihre Nachrichten nicht erhalten, können sie nicht sehen, geschweige denn, mit ihnen interagieren.

Die Reputation des Senders hat auf der Ebene des Kundenerlebnisses den größten Einfluss auf die Posteingangszustellbarkeit. Sie bestimmt, ob unerwünschte Nachrichten die Empfänger erreichen oder ob benötigte Nachrichten zum Spam-Ordner weitergeleitet oder blockiert werden, bevor sie die Möglichkeit haben, die Postfächer der Empfänger zu erreichen.

Wie der virtuelle Zustellbarkeitsmanager dazu beitragen kann, die Zustellbarkeit und die Reputation zu verbessern

Der virtuellen Zustellbarkeitsmanager hilft Ihnen dabei, sowohl Ihre Zustellbarkeit als auch Ihre Reputation zu verbessern. Er verfügt über ein Dashboard, das sowohl allgemeine als auch detaillierte Ansichten des E-Mail-Programms Ihres Kontos bietet, damit Sie sich auf problematische Bereiche konzentrieren können, und einen Berater, der Lösungen zur Behebung bereitstellt, um Infrastrukturprobleme zu beheben, die sich negativ auf die Zustellbarkeit und den Ruf Ihrer E-Mails auswirken.

- Dashboard – bietet Einblicke in Ihre Zustellbarkeitsdaten mit Schwerpunkt auf den Ebenen „Konto“, „ISP“, „Sendeidentität“ und „Konfigurationssatz“. Auf diese Weise können Sie problematische Bereiche und Trends schnell erkennen und Probleme abfangen, bevor sie zu größeren Zustellungsproblemen wie vorübergehenden Ablehnungen (Verzögerungen) oder Sperren führen. Diese Erkenntnisse helfen Ihnen auch dabei, Ihre Reputation als Absender zu verbessern, indem Sie die idealen Zeiten und Datumsangaben für eine bessere Kundenbindung und Konversionen für Ihre E-Mail-Kampagnen berechnen.

- Berater – bietet Empfehlungen zur Verbesserung Ihres E-Mail-Versands, indem Konfigurationsprobleme gemeldet werden, die sich negativ auf Ihre E-Mail-Zustellbarkeit und Ihre Reputation auswirken. Er empfiehlt Lösungen zur Behebung bestimmter Probleme in der Infrastruktur Ihrer Sendedomäne, Ihres IP-Bereichs und Ihrer Authentifizierungsdatensätze, z. B. wenn SPF-, DMARC- oder DKIM-Datensätze nicht vorhanden sind oder eine DKIM-Schlüssellänge zu kurz ist.

Erste Schritte mit dem virtuellen Zustellbarkeitsmanager

Wenn Sie mit der Verwendung des virtuellen Zustellbarkeitsmanagers beginnen möchten, führt Sie ein Onboarding-Assistent in der Amazon-SES-Konsole durch die Schritte zur Aktivierung von Virtual Deliverability Manager für Ihr Konto. Siehe the section called “Erste Schritte”.

Themen

- Erste Schritte mit dem virtuellen Zustellbarkeitsmanager
- Dashboard des virtuellen Zustellbarkeitsmanagers
- Berater für den virtuellen Zustellbarkeitsmanager
- Einstellungen des virtuellen Zustellbarkeitsmanagers

Erste Schritte mit dem virtuellen Zustellbarkeitsmanager

Wenn Sie den virtuellen Zustellbarkeitsmanager mit Ihrem Konto verwenden möchten, müssen Sie ihn mithilfe des Onboarding-Assistenten in der Amazon-SES-Konsole aktivieren. Dort richten Sie die Interaktionsnachverfolgung und optimierte gemeinsame Zustellung ein. Der virtuelle Zustellbarkeitsmanager nutzt die Interaktionsnachverfolgung und optimierte gemeinsame Zustellung, um Ihre Sendungen zu überwachen und Ihnen zu helfen, Ihre Zustellbarkeit und Ihre Reputation zu verbessern.

- Interaktionsnachverfolgung – die Fähigkeit, das Interaktionsverhalten der Empfänger anhand von Öffnungs- und Klickereignissen zu überwachen, indem ein Tracking-Pixel in einem verpackten Link verwendet wird. Bei Auslösung zeigt das Tracking-Pixel einen Zeitstempel an, wann eine Nachricht geöffnet wurde, und gibt an, auf welche Links der Empfänger geklickt hat. Wenn Sie diese Option aktivieren, werden Ihre URLs Links so geändert, dass sie Amazon SES SES-Engagement-Tracking-Wrapper enthalten.

- Optimierte gemeinsame Zustellung – wählt automatisch die optimale IP-Adresse für den E-Mail-Versand aus und verbessert so die Endpunktzustellung von Nachrichten an die E-Mail-Zielempfänger.

Sowohl die Interaktionsnachverfolgung als auch die optimierte gemeinsame Zustellung sind im Onboarding-Assistenten standardmäßig aktiviert, Sie haben jedoch die Möglichkeit, sie zu deaktivieren. Wir empfehlen dringend, beide Funktionen aktiviert zu lassen, um den virtuellen Zustellbarkeitsmanager optimal nutzen zu können.

Erste Schritte mit dem virtuellen Zustellbarkeitsmanager bei Verwendung der Amazon-SES-Konsole

Die folgende Vorgehensweise zeigt Ihnen die ersten Schritte mit dem virtuellen Zustellbarkeitsmanager bei Verwendung der Amazon-SES-Konsole.

So beginnen Sie den virtuellen Zustellbarkeitsmanager mit der Amazon-SES-Konsole zu verwenden

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich den virtuellen Zustellbarkeitsmanager aus.
3. Wählen Sie auf der Seite Virtual Deliverability Manager overview (Übersichtsseite des virtuellen Zustellbarkeitsmanagers) eine der Schaltflächen Get started with Virtual Deliverability Manager (Erste Schritte mit dem virtuellen Zustellbarkeitsmanager) aus.
4. Akzeptieren Sie auf der Seite Select Engagement tracking (Interaktionsnachverfolgung auswählen) die Standardeinstellung oder Turn off engagement tracking (Interaktionsnachverfolgung deaktivieren) und anschließend Next (Weiter) aus.

   > **Note**
   >
   > Wenn Sie die Interaktionsverfolgung aktivieren, werden Ihre Links URLs und Ihre Links so geändert, dass sie Amazon SES SES-Engagement-Tracking-Wrapper enthalten.

5. Akzeptieren Sie auf der Seite Select Optimized shared delivery (Optimierte gemeinsame Zustellung auswählen) die Standardeinstellung oder wählen Sie Turn off optimized shared delivery (Optimierte gemeinsame Zustellung deaktivieren) und anschließend Next (Weiter) aus.

> **Important**
>
> Eine optimierte gemeinsame Zustellung kann zu präventiven Verzögerungen beim Senden Ihrer E-Mails führen, um Ihre Reputation als Absender zu schützen. Bei einer kritischen Workload, der unverzüglich gesendet werden muss, empfehlen wir Ihnen, diese Einstellung nicht zu aktivieren. Verwenden Sie stattdessen Konfigurationssätze für das Senden und aktivieren Sie die optimierte gemeinsame Zustellung nur für die Konfigurationssätze, bei denen Sie sich Verzögerungen leisten können.

6. Auf der Seite Review and enable (Überprüfen und aktivieren) können Sie Ihre Optionen für die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung überprüfen. Wählen Sie Previous (Zurück), wenn Sie zurückkehren und Änderungen vornehmen möchten. Andernfalls wählen Sie Enable Virtual Deliverability Manager (Virtueller Zustellbarkeitsmanager aktivieren) aus.

   Die Seite mit den Einstellungen des virtuellen Zustellbarkeitsmanagers wird geöffnet. Im Bereich Subscription overview (Abonnementübersicht) wird der Status des virtuellen Zustellbarkeitsmanagers angezeigt, und im Bereich Additional settings (Zusätzliche Einstellungen) wird der Status von Engagement Tracking (Interaktionsnachverfolgung) sowie Optimized Shared Delivery (Optimierte gemeinsame Zustellung) angezeigt.

Sobald Sie den virtuellen Zustellbarkeitsmanager für Ihr Konto aktiviert haben, können Sie benutzerdefinierte Einstellungen dafür definieren, wie ein Konfigurationssatz die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung verwendet, indem Sie die im virtuellen Zustellbarkeitsmanager definierten Einstellungen überschreiben. Damit erhalten Sie die Flexibilität, Ihren E-Mail-Versand an bestimmte E-Mail-Kampagnen anzupassen. Sie können beispielsweise die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung für Ihre Marketing-E-Mails aktivieren und für Ihre Transaktions-E-Mail deaktivieren. Sehen Sie sich beim Erstellen oder Bearbeiten eines Konfigurationssatzes die Optionen des virtuellen Zustellbarkeitsmanagers an.

Erste Schritte mit Virtual Deliverability Manager mithilfe des AWS CLI

Die folgende Vorgehensweise zeigt Ihnen die ersten Schritte mit dem virtuellen Zustellbarkeitsmanager unter Verwendung der AWS CLI.

Um mit Virtual Deliverability Manager zu beginnen, verwenden Sie den AWS CLI

Sie können die PutAccountVdmAttributes-Operation in der Amazon-SES-API v2 für die ersten Schritte mit virtuellen Zustellbarkeitsmanager verwenden. Sie können diesen Vorgang von der aus aufrufen AWS CLI, wie in den folgenden Beispielen gezeigt.

- Aktivieren Sie den virtuellen Zustellbarkeitsmanager in Ihrem Konto:

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --vdm-attributes
 VdmEnabled=ENABLED
```

- Aktivieren Sie sowohl die Interaktionsnachverfolgung als auch die optimierte gemeinsame Zustellung mithilfe einer Eingabedatei:

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --cli-input-json file://
attributes.json
```

  Die Eingabedatei sieht in etwa wie folgt aus:

```
{
    "VdmAttributes": {
        "VdmEnabled": "ENABLED",
        "DashboardAttributes": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianAttributes": {
            "OptimizedSharedDelivery": "ENABLED"
        }
    }
}
```

  Parameterwerte und zugehörige Datentypen können durch eine Verknüpfung mit dem VdmAttributes-Datentyp in der Referenz für Amazon-SES-API v2 gefunden werden.

> **Note**
>
> Wenn Sie die Interaktionsverfolgung aktivieren, werden Ihre Links URLs und Ihre Links so geändert, dass sie Amazon SES SES-Engagement-Tracking-Wrapper enthalten.

> **Important**
>
> Eine optimierte gemeinsame Zustellung kann zu präventiven Verzögerungen beim Senden Ihrer E-Mails führen, um Ihre Reputation als Absender zu schützen. Bei einer kritischen Workload, der unverzüglich gesendet werden muss, empfehlen wir Ihnen, diese Einstellung nicht zu aktivieren. Verwenden Sie stattdessen Konfigurationssätze für das Senden und aktivieren Sie die optimierte gemeinsame Zustellung nur für die Konfigurationssätze, bei denen Sie sich Verzögerungen leisten können.

- So überprüfen Sie das Ergebnis:

```
aws --region us-east-1 sesv2 get-account
```

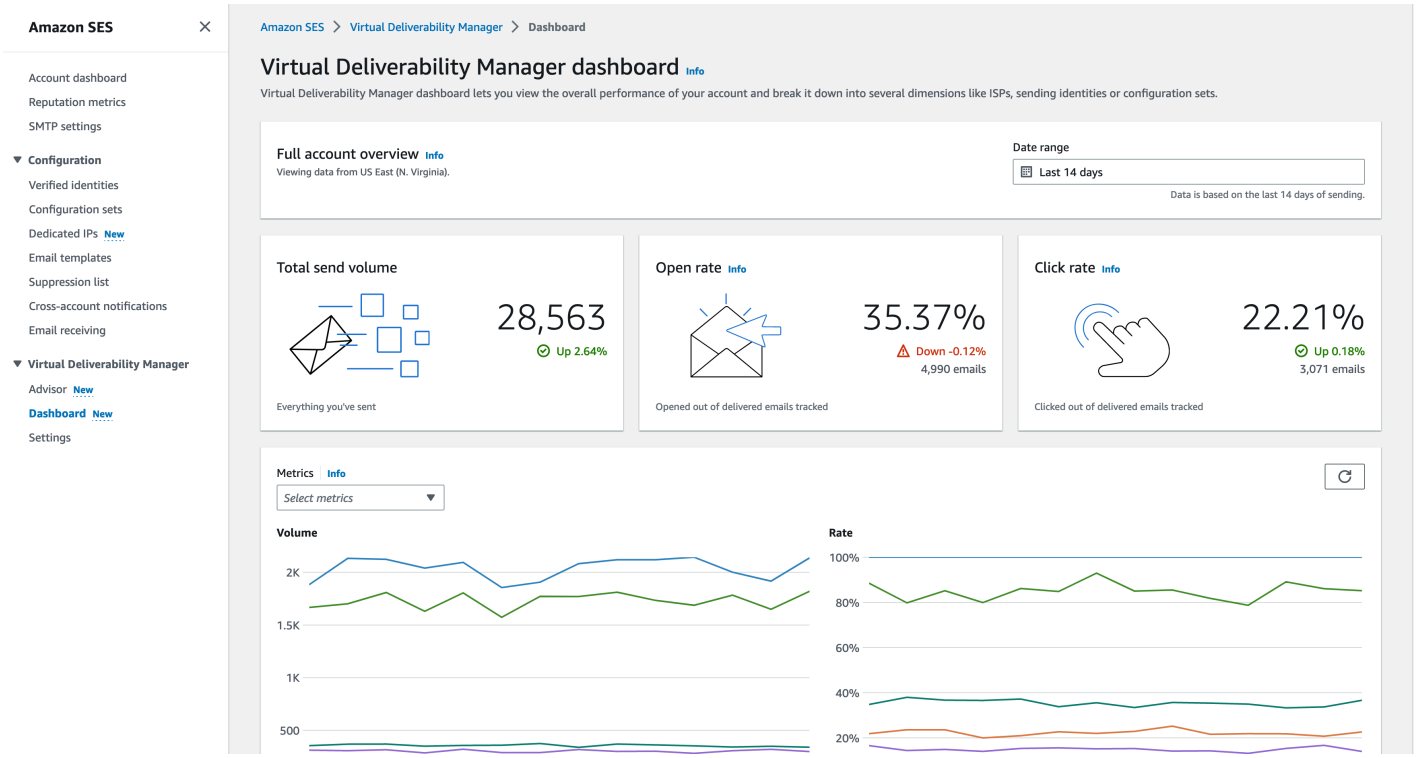
- Um benutzerdefinierte Einstellungen dafür zu definieren, wie ein Konfigurationssatz das Engagement-Tracking und die optimierte gemeinsame Lieferung verwendet, indem die in Virtual Deliverability Manager definierten Einstellungen außer Kraft gesetzt werden, finden Sie im Beispiel unter. AWS CLI the section called “Einstellungen”

Dashboard des virtuellen Zustellbarkeitsmanagers

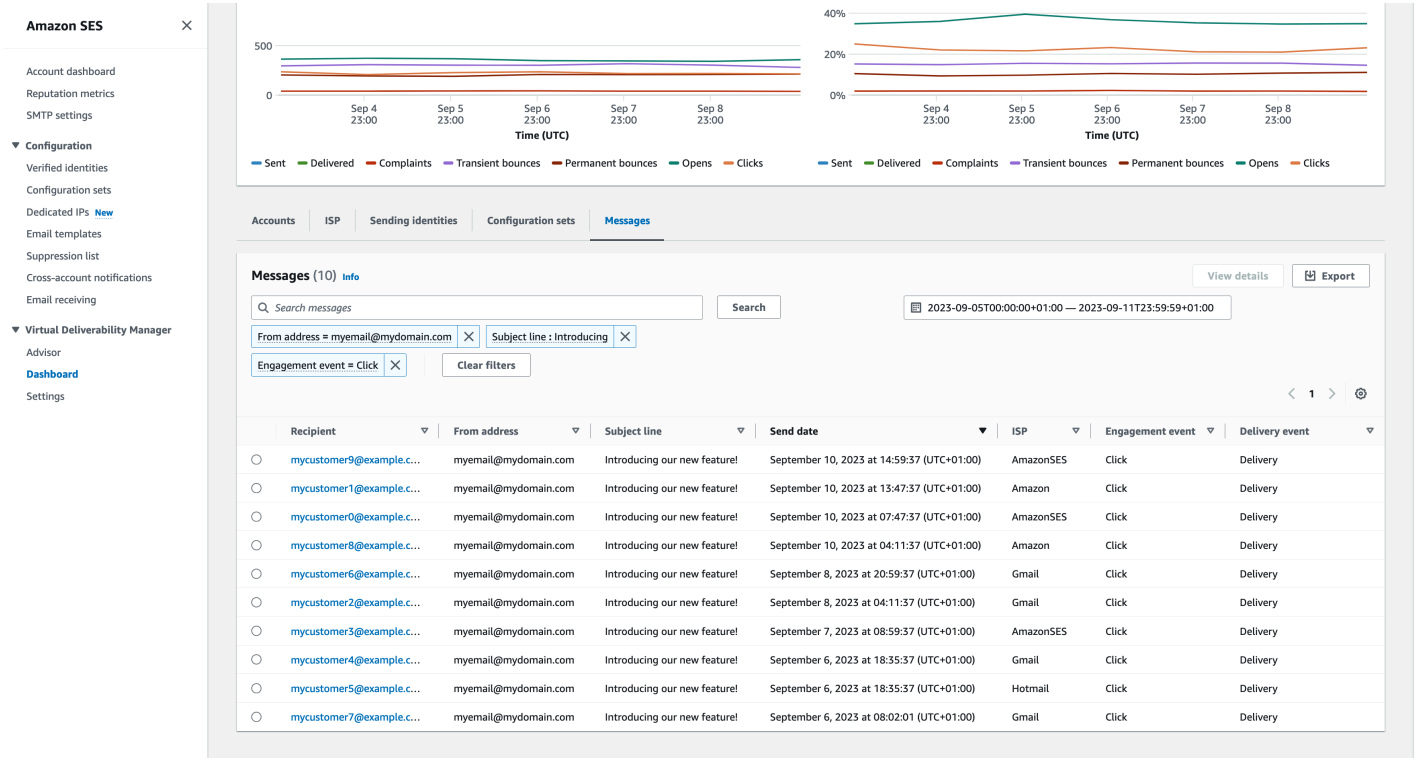
Das Dashboard bietet allgemeine Ansichten des Zustellbarkeitsprogramms Ihres Kontos, z. B. leicht lesbare Karten und Zeitreihendiagramme, die die Zustellbarkeit und den Ruf anhand von Lieferraten open/click und bounce/complaint Statistiken aufzeigen. Das Dashboard bietet auch eine detailliertere Ansicht, sodass Sie detailliertere spezifische Tabellendaten aufrufen können, wenn es ein Problem gibt, das mit einem bestimmten mit einer E-Mail-Kampagne verknüpften ISP, einer bestimmten Sendeidentität oder einem Konfigurationssatz zusammenhängt.

Mit der Möglichkeit, die Dinge von einem allgemeinen Standpunkt aus zu betrachten und auch spezifische Details anzuzeigen, können Sie sich auf die problematischen Bereiche der Zustellbarkeit konzentrieren, anstatt Ihr E-Mail-Programm als Ganzes überprüfen zu müssen. Dank dieses umfassenden Einblicks können Sie auch Trends abfangen und mögliche Probleme erkennen, bevor sie zu größeren Problemen bei der Zustellbarkeit wie Verzögerungen oder Blockaden führen.

Eine Kontoübersicht im Dashboard von Virtual Deliverability Manager mit den Karten und Zeitreihendiagrammen.



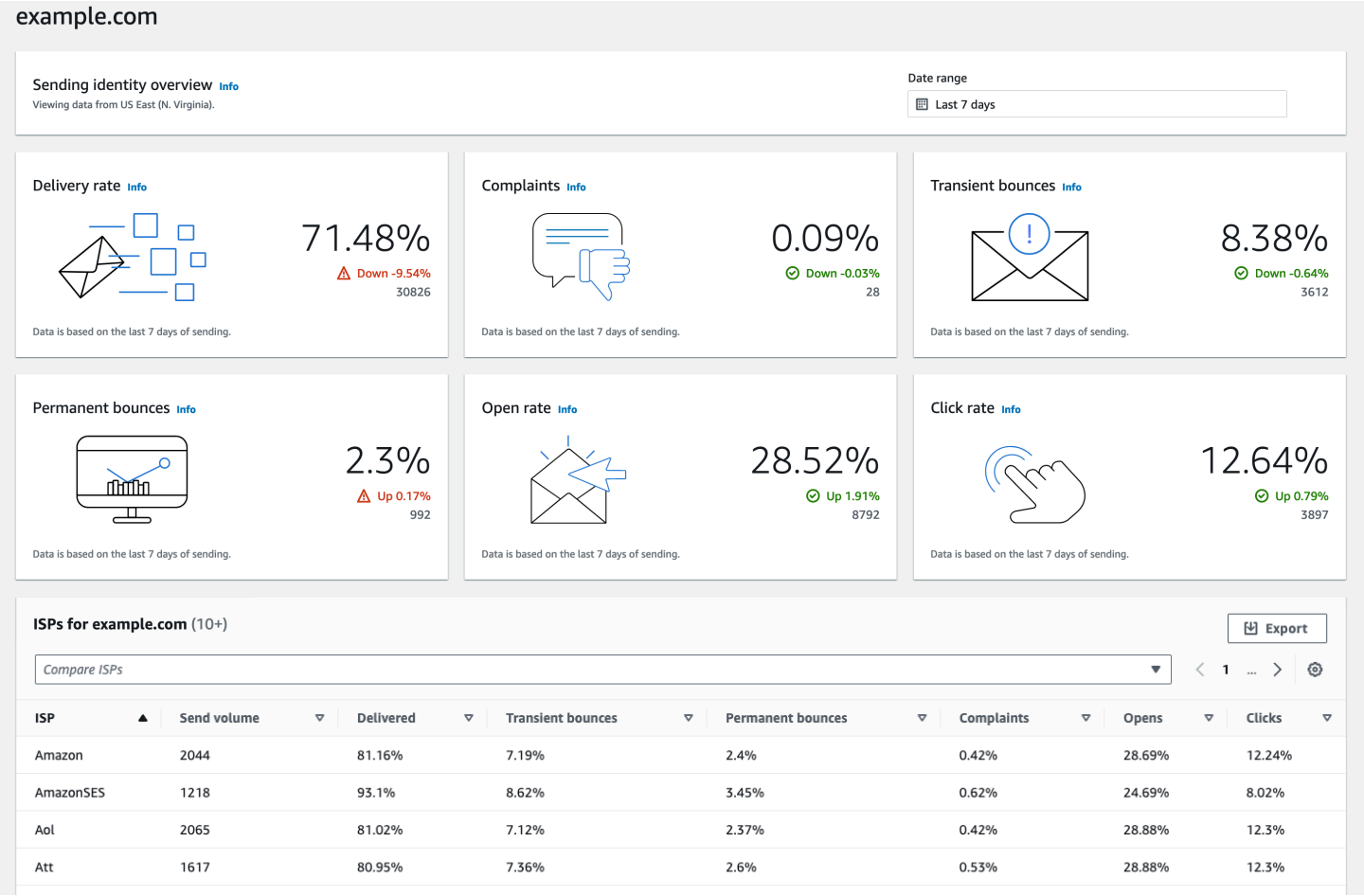
Die im Dashboard von Virtual Deliverability Manager ausgewählte Tabelle Nachrichten enthält gesendete Nachrichten, die dem Zeitraum und den Filterkriterien entsprechen.



Granulare Daten, die vom Dashboard bereitgestellt werden, können Ihnen helfen, Ihre Reputation als Absender zu verbessern und die idealen Zeiten und Daten für eine bessere Interaktion und Konversionen für Ihr E-Mail-Programm zu berechnen, wobei Sie die Möglichkeit haben, bestimmte Datensätze detaillierter anzuzeigen:

- ISP-Daten – wertvoll bei einem Problem mit der Zustellbarkeit eines bestimmten ISP oder Postfachanbieters – anstatt zu versuchen, Ihr gesamtes Konto anzupassen, was sonst möglicherweise gut läuft, können Sie sich auf den problematischen Endpunkt konzentrieren und sich an dessen bewährten Methoden orientieren, um die Reputation des Absenders bei diesem ISP zu verbessern und eine gute Posteingangszustellung wiederherzustellen, sodass Sie Ihre Empfänger erreichen. Es ist auch wichtig, Ihre ISP-Verteilung zu verstehen, da Sie möglicherweise mehr an einen ISP oder Postfachanbieter senden als an andere. Sie müssen sicherstellen, dass der Datenverkehr immer zugestellt und von den Endempfängern genutzt wird, damit er sich positiv auf Ihre E-Mail-Konversion auswirkt.
- Sendeidentitäts- und Konfigurationssatzdaten – hilft Ihnen dabei, Sendeidentitäten und Konfigurationssätze zu identifizieren, die zu Ihrem allgemeinen Problem mit der Zustellbarkeit Ihres Kontos beitragen. Sie können sich gezielt auf diese konzentrieren, Ihre Konfigurationen anpassen und möglicherweise das Senden mit einer bestimmten Identität reduzieren, bis das Problem behoben ist. Beispielsweise wird eine Sendeidentität versehentlich an eine Unterdrückungsliste gesendet, sodass der gesamte Datenverkehr über diese Identität geleitet wird. Diese Identität ist mit einem Konfigurationssatz verknüpft, was zu Problemen mit der Zustellbarkeit führt. In solchen Fällen ist es von Vorteil, die Sendeidentität oder den Konfigurationssatz identifizieren zu können, sodass Sie sich darauf konzentrieren können, dieses Problem gezielt zu beheben, anstatt Ihr gesamtes Konto durchsuchen zu müssen, um die Ursache für das Zustellbarkeitsproblem zu ermitteln.

Detaildaten werden im Dashboard von Virtual Deliverability Manager für die ausgewählte Sendeidentität, example.com, angezeigt. Auf Karten werden Metriken zur Zustellbarkeit und Reputation angezeigt. In der Tabelle werden alle Empfänger angezeigt, an ISPs die der Absender E-Mails gesendet hat, mit Kennzahlen für jeden Internetdienstanbieter innerhalb des eingegebenen Zeitraums.



Verwenden des Dashboards des virtuellen Zustellbarkeitsmanagers in der Amazon-SES-Konsole

Das folgende Verfahren zeigt Ihnen, wie Sie das Virtual-Deliverability-Manager-Dashboard in der Amazon-SES-Konsole verwenden, um Ihre allgemeinen Statistiken zur Zustellbarkeit und zur Reputation einzusehen und problematische Bereiche genauer zu untersuchen.

Mit dem Dashboard des virtuellen Zustellbarkeitsmanagers können Sie sich allgemeine und detailliertere Metriken zur Zustellbarkeit Ihres Kontos ansehen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Virtual Deliverability Manager (Virtueller Zustellbarkeitsmanager) die Option Dashboard aus.

> **Note**
>
> - Das Dashboard wird nicht angezeigt, wenn Sie den virtuellen Zustellbarkeitsmanager nicht für Ihr Konto aktiviert haben. Weitere Informationen finden Sie unter the section called “Erste Schritte”.
> - Dashboard-Kennzahlen werden nahezu in Echtzeit angezeigt.
> - Dashboard-Nachrichten werden innerhalb weniger Minuten nach dem Versand angezeigt.

3. Wählen Sie im Bereich Vollständige Kontoübersicht einen Zeitraum aus, der für alle Metriken in den Karten, Zeitreihendiagrammen und Detailtabellen verwendet werden soll.

- Wählen Sie im Feld Date range (Datumsbereich) die Option Relative range (Relativer Bereich) (Standard) oder Absolute range (Absoluter Bereich).
  - Relative range (Relativer Bereich) – wählen Sie das Optionsfeld aus, das der Anzahl der gewünschten Tage entspricht.
    - Benutzerdefinierter Bereich – geben Sie einen Zeitraum in Tagen (bis zu 60), Wochen (bis zu 8) oder 2 Monaten ein.
  - Absoluter Bereich – das erste Datum, das Sie auswählen, ist das Startdatum, das zweite Datum ist das Enddatum und insgesamt 60 Tage dürfen nicht überschritten werden. Wenn Sie einen einzelnen Tag angeben möchten, wählen Sie ihn sowohl für das Startdarum als auch für das Enddatum aus.

> **Note**
>
> Folgendes gilt für alle Datumsbereiche im Dashboard:
>
> - Alle Daten und Zeiten werden in UTC angegeben.
> - Bei Datumsangaben im Relative range (relativen Bereich) endet der letzte Tag mit einem Zeitstempel um Mitternacht UTC. Wenn Sie beispielsweise Letzte 7 Tage auswählen, wäre der siebte Tag gestern mit einem Ende um Mitternacht.

- Wenn der Zeitraum länger als 30 Tage ist, haben die Spalte % Differenz in der Tabelle Kontostatistiken und die Änderungsprozentsätze in den Karten keinen Wert (durch einen Bindestrich - gekennzeichnet).

4. Die Karten, Zeitreihendiagramme und alle Detailtabellen, d. h. Kontenstatistiken, ISP, Sendeidentitäten und Konfigurationssätze, zeigen metrische Summen an, die anhand des eingegebenen Datumsbereichs berechnet wurden, und verwenden die in So werden Dashboard-Metriken berechnet beschriebene metrische Mathematik.

   - Um eine lokale `.csv`-Datei mit den Daten zu erstellen, die Sie gerade in der Tabelle ISP, Sendeidentitäten oder Konfigurationssätze anzeigen, klicken Sie auf die entsprechende Schaltfläche Exportieren.

5. Zeitreihendiagramme, die den Fortschritt bei Volumen und Rate für den von Ihnen eingegebenen Zeitraum darstellen, werden im Bereich Metriken angezeigt. Wenn Sie in den Grafiken den Mauszeiger über ein Datumsintervall bewegen, wird die genaue Volumenzahl oder der Prozentsatz der Rate auf der Grundlage einer täglichen Aggregation angezeigt. Sie können die Metriken, die Sie sehen möchten, mithilfe der Dropdown-Liste Metriken auswählen filtern.

6. Wählen Sie die Registerkarte Accounts (Konten) aus, um die Tabelle mit den Accounts statistics (Kontostatistiken) anzuzeigen.

   - Diese Tabelle bietet einen Überblick über die Metriken zur Zustellbarkeit und zur Reputation und zeigt Total Volume (Gesamtvolumen), % Rate (Rate in %) und % Difference (Differenz in %) für Sent (Gesendet), Delivered (Zugestellt), Complaints (Beschwerden), Transient & Permanent bounces (Vorübergehende und permanente Unzustellbarkeit) sowie Opens & Clicks (Öffnungen und Klicks), die anhand des eingegebenen Datumsbereichs berechnet wurden.

   > **Note**
   >
   > Wenn der Datumsbereich mehr als 30 Tage beträgt, enthält die Spalte % Differenz keinen Wert (durch einen Bindestrich - gekennzeichnet).

7. Wählen Sie die Registerkarte ISP aus, um die ISP-Tabelle anzuzeigen.

   - In dieser Tabelle werden für jeden ISP, an den Sie gesendet haben, anhand des eingegebenen Datumsbereichs die Werte für Send volume (Sendevolumen), Delivered (Zugestellt), Transient & Permanent bounces (Vorübergehende und permanente

Unzustellbarkeit), Complaints (Beschwerden), Opens & Clicks (Öffnungen und Klicks) berechnet.

- Um gezielt zu filtern ISPs, aktivieren Sie im ISPs Suchfeld Vergleichen das entsprechende Kontrollkästchen für jeden ISP, den Sie einbeziehen möchten.
- Um eine lokale `.csv`-Datei mit den Daten zu erstellen, die Sie gerade in dieser Tabelle anzeigen, wählen Sie die entsprechende Schaltfläche Exportieren.

8. Wählen Sie die Registerkarte Sending identities (Sendeidentitäten) aus, um die Tabelle Sending identities (Sendeidentitäten) anzuzeigen.

   - In dieser Tabelle werden für jede Sendeidentität, die Sie verwendet haben, anhand des eingegebenen Datumsbereichs die Werte für Send volume (Sendevolumen), Delivered (Zugestellt), Transient & Permanent bounces (Vorübergehende und permanenten Unzustellbarkeit), Complaints (Beschwerden), Opens & Clicks (Öffnungen und Klicks) berechnet.
   - Wenn Sie bestimmte Sendeidentitäten filtern möchten, markieren Sie im Suchfeld Identitäten auswählen das entsprechende Kontrollkästchen für jeden einzubeziehenden ISP.
   - Wenn Sie eine bestimmte Sendeidentität genauer untersuchen möchten, wählen Sie ihren Namen in der Spalte Sending identity (Sendeidentität) aus.
     - Es werden Karten mit Zustellungsrate, Beschwerden, Vorübergehende und Permanente Unzustellbarkeiten, Öffnungs- und Klickrate für die ausgewählte Sendeidentität angezeigt, die anhand des eingegebenen Datumsbereichs berechnet wurden.
     - Die Zeitreihendiagramme werden aktualisiert und zeigen alle Metriken für die ausgewählte Sendeidentität an, und zwar berechnet anhand des eingegebenen Datumsbereichs.
     - Es wird eine ISP-Tabelle angezeigt, in der alle Absenderidentitäten aufgeführt sind, an ISPs die E-Mails gesendet wurden, mit Metriken für jeden ISP, die anhand des eingegebenen Datumsbereichs berechnet wurden.
   - Um eine lokale `.csv`-Datei mit den Daten zu erstellen, die Sie gerade in dieser Tabelle anzeigen, wählen Sie die entsprechende Schaltfläche Exportieren.

9. Wählen Sie die Registerkarte Configuration sets (Konfigurationssätze) aus, um die Tabelle Configuration sets (Konfigurationssätze) anzuzeigen.

   - In dieser Tabelle werden für jeden Konfigurationssatz, der zum Versenden von E-Mails verwendet wurde, anhand des eingegebenen Datumsbereichs die Werte für Send volume (Sendevolumen), Delivered (Zugestellt), Transient & Permanent bounces (Vorübergehende

und permanenten Unzustellbarkeit), Complaints (Beschwerden), Opens & Clicks (Öffnungen und Klicks) berechnet.

- Wenn Sie bestimmte Konfigurationssätze filtern möchten, markieren Sie im Suchfeld Konfigurationssätze vergleichen das entsprechende Kontrollkästchen für jeden einzubeziehenden Konfigurationssatz.
- Wenn Sie einen bestimmten Konfigurationssatz genauer untersuchen möchten, wählen Sie dessen Namen in der Spalte Configuration set (Konfigurationssatz) aus.
  - Es werden Karten mit Zustellungsrate, Beschwerden, Vorübergehende und Permanente Unzustellbarkeiten, Öffnungs- und Klickrate für den ausgewählten Konfigurationssatz angezeigt, die anhand des eingegebenen Datumsbereichs berechnet wurden.
  - Die Zeitreihendiagramme werden aktualisiert und zeigen alle Metriken für den ausgewählten Konfigurationssatz an, und zwar berechnet anhand des eingegebenen Datumsbereichs.
  - Es wird eine ISP-Tabelle angezeigt, in der die gesamte Konfiguration aufgeführt ist, an ISPs die E-Mails gesendet wurden, mit Metriken für jeden ISP, die anhand des eingegebenen Datumsbereichs berechnet wurden.
- Um eine lokale `.csv`-Datei mit den Daten zu erstellen, die Sie gerade in dieser Tabelle anzeigen, wählen Sie die entsprechende Schaltfläche Exportieren.

10. Wählen Sie die Registerkarte Nachrichten aus, um die Tabelle Nachrichten anzuzeigen.

    Dies ist eine interaktive Tabelle, mit der Sie Ihre gesendeten Nachrichten suchen und finden können. Für jede Nachricht können Sie den aktuellen Zustellungs- und Kontaktstatus sowie den Ereignisverlauf verfolgen und die vom Postfachanbieter zurückgegebene Antwort einsehen. Die folgenden Punkte decken ab, wie Sie nach bestimmten Nachrichten suchen können:

    - Wenn Sie in der Datumsauswahl eine Auswahl treffen, können Sie nach Nachrichten filtern, die Sie in den letzten 30 Tagen gesendet haben. Wenn Sie keinen Datumsbereich auswählen, wird die Suche standardmäßig auf die letzten 7 Tage einschließlich des aktuellen Tages in Ihrer Zeitzone angewendet.
    - Im Feld Nachrichten suchen können Sie nach Empfänger, Absenderadresse, Betreffzeile, ISP, Benutzerbindungsereignisse, Zustellungsereignis und ID filtern. Es gelten die folgenden Eigenschaften:
      - Je nach Filtertyp geben Sie entweder eine Zeichenfolge ein, bei der Groß- und Kleinschreibung beachtet wird, oder Sie wählen einen Wert aus einer Liste aus.
      - Das Benutzerbindungsereignis ist auf einen einzigen Wert beschränkt, die Betreffzeile kann bis zu zwei Werte enthalten, und alle anderen Filter können bis zu fünf Werte pro Suche

enthalten. Die Filterung nach Nachrichten-ID schließt alle anderen Filter aus, die Sie möglicherweise ausgewählt haben, auch den Datumsbereich.

- Die Spalte Nachrichten-ID ist standardmäßig ausgeblendet, kann aber angezeigt werden, indem Sie auf das Zahnradsymbol klicken, um die Anzeige der Tabelle Nachrichten anzupassen.

- Nachdem Sie Ihre Filter und den Datumsbereich ausgewählt haben, wählen Sie Suchen aus. Daraufhin wird die Tabelle mit Nachrichten gefüllt, die Ihren Suchkriterien entsprechen. Die Tabelle kann bis zu 100 Nachrichten laden. Wenn Ihre Suche mehr als 100 Nachrichten zurückgibt, sind die 100 Nachrichten in der Tabelle eine Zufallsstichprobe der insgesamt zurückgegebenen Nachrichten.
- Wenn Sie das Optionsfeld einer Nachricht und anschließend Details anzeigen auswählen, wird die Seitenleiste Informationen zur Nachricht angezeigt. Sie enthält Informationen zum vollständigen Ereignisverlauf der Nachricht, mit dem neuesten Ereignis ganz oben, sowie zu allen Antworten oder Diagnosecodes, die vom Postfachanbieter zurückgegeben wurden.
- Um eine lokale `.csv`-Datei mit den Daten zu erstellen, die Sie gerade in dieser Tabelle anzeigen, wählen Sie die entsprechende Schaltfläche Exportieren.

Zugreifen auf Ihre Virtual Deliverability Manager-Metrikdaten mithilfe der AWS CLI

Die folgenden Beispiele zeigen Ihnen, wie Sie mithilfe der AWS CLI auf die Empfehlungen des virtuellen Zustellbarkeitsmanagers zugreifen. Dies sind dieselben Daten, die in der Konsole im Dashboard des virtuellen Zustellbarkeitsmanagers in der Amazon-SES-Konsole.

Um auf Ihre Messdaten zur Zustellbarkeit zuzugreifen, verwenden Sie den AWS CLI

Sie können mit dem `BatchGetMetricData`-Vorgang in der Amazon-SES-API v2 Ihre Empfehlungen auflisten. Sie können diesen Vorgang, wie in den folgenden Beispielen dargestellt, von der AWS CLI aus aufrufen.

- Greifen Sie auf Ihre Metrikdaten zur Zustellbarkeit:

```
aws --region us-east-1 sesv2 batch-get-metric-data --cli-input-json file://sends.json
```

- Die Eingabedatei sieht in etwa wie folgt aus:

```
{
```

```
 "Queries": [
   {
     "Id": "Retrieve-Account-Sends",
     "Namespace": "VDM",
     "Metric": "SEND",
     "StartDate": "2022-11-04T00:00:00",
     "EndDate": "2022-11-05T00:00:00"
    }
 ]
}
```

Weitere Informationen über Parameterwerte und zugehörige Datentypen finden Sie durch eine Verknüpfung mit dem `BatchGetMetricDataQuery`-Datentyp in der Referenz für Amazon-SES-API v2.

Filtern und Exportieren Ihrer Messdaten zur Zustellbarkeit mithilfe der AWS CLI

Dieses Beispiel veranschaulicht, wie Sie den `CreateExportJob`-Vorgang verwenden, um Ihre Metikdaten zur Zustellbarkeit mithilfe der AWS CLI zu filtern und in eine CSV- oder JSON-Datei zu exportieren. Dies sind dieselben Daten, die auch in den Tabellen ISP, Senden von Identitäten und Konfigurationssätze im Virtual-Deliverability- Manager-Dashboard verwendet werden.

Um Ihre Messdaten zur Zustellbarkeit zu filtern und in eine .csv- oder .json-Datei zu exportieren, verwenden Sie den AWS CLI

Sie können die Operation `CreateExportJob` zusammen mit dem Datentyp `MetricsDataSource`in Amazon SES API v2 verwenden, um Ihre Metrikdaten zu filtern und in eine CSV- oder JSON-Datei zu exportieren. Sie rufen diesen Vorgang von der aus auf, AWS CLI wie im folgenden Beispiel gezeigt.

- Filtern und exportieren Sie Ihre Metrikdaten zur Zustellbarkeit mithilfe einer Eingabedatei:

```
aws --region us-east-1 sesv2 create-export-job --cli-input-json file://metric-export-input.json
```

- In diesem Beispiel verwendet die Eingabedatei `MetricsDataSource`Parameter, um nach allen E-Mails zu filtern, an die ISPs Sie gesendet haben. Dabei wird die Rate der erfolgreichen Zustellung

innerhalb des angegebenen Datumsbereichs und das für die Ausgabedatei angegebene CSV-Format angezeigt:

```
{
    "ExportDataSource": {
        "MetricsDataSource": {
            "Dimensions": {
                "ISP": ["*"]
            },
            "Namespace": "VDM",
            "Metrics": [
                {
                    "Name": "DELIVERY",
                    "Aggregation": "RATE"
                }
            ],
            "StartDate": "2023-06-13T00:00:00",
            "EndDate": "2023-06-20T00:00:00"
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

Weitere Informationen über Parameterwerte und zugehörige Datentypen finden Sie in `MetricsDataSource` als ein Objekt des Typs `ExportDataSource` in der Referenz für Amazon-SES-API v2.

Finden Sie Ihre gesendeten Nachrichten, ihren Liefer- und Interaktionsstatus und exportieren Sie die Ergebnisse mithilfe der AWS CLI

In diesen Beispielen wird veranschaulicht, wie Sie bestimmte Nachrichten, die Sie gesendet haben, mithilfe der `CreateExportJob` suchen und finden, deren aktuellen Zustellungs- und Interaktionsstatus anzeigen und die Ergebnisse der Suche in eine CSV- oder JSON-Datei exportieren können. Verwenden Sie dazu die AWS CLI. Dies sind dieselben Daten, die in der Tabelle Nachrichten des Virtual-Deliverability-Manager-Dashboards verwendet werden.

Um nach gesendeten Nachrichten, ihrem Zustell- und Interaktionsstatus zu suchen und die Ergebnisse in eine CSV- oder JSON-Datei zu exportieren, verwenden Sie den AWS CLI

Sie können die `CreateExportJob`-Operation zusammen mit dem `MessageInsightsDataSource`-Datentyp in Amazon SES API v2 verwenden, um unter Anwendung von Filtern bestimmte gesendete Nachrichten zu suchen, deren Zustellungs- und Interaktionsstatus zu überprüfen und die Ergebnisse in eine CSV- oder JSON-Datei zu exportieren. Sie rufen diesen Vorgang von der aus auf, AWS CLI wie in den folgenden Beispielen gezeigt.

> **Note**
>
> Wenn Ihre gefilterte Suche mehr als 10 000 Nachrichten zurückgibt, sind die 10 000 Nachrichten in API-Ergebnissatz eine Zufallsstichprobe der insgesamt zurückgegebenen Nachrichten.

- Suchen Sie nach gesendeten Nachrichten, sehen Sie sich deren aktuellen Status an und exportieren Sie die Ergebnisse mithilfe einer Eingabedatei:

```
aws --region us-east-1 sesv2 create-export-job --cli-input-json file://message-insights-export-input.json
```

- In diesem Beispiel verwendet die Eingabedatei `MessageInsightsDataSource`-Parameter, um nach einem Thema zu filtern, das „Aktion endet heute!“ entspricht, und ein für die Ausgabedatei angegebenes CSV-Format:

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Sale Ends Tonight!"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

- In diesem Beispiel verwendet die Eingabedatei `MessageInsightsDataSource`Parameter, um nach einem Betreff zu filtern, der mit „Hello“ beginnt, mit einer FromEmailAddress „Information“ an Ziele gesendet wird, die mit „@example .com“ enden, und einem für die Ausgabedatei angegebenen JSON-Format:

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Hello*"
                ],
                "FromEmailAddress": [
                    "*information*"
                ],
                "Destination": [
                    "*@example.com"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "JSON"
    }
}
```

- In diesem Beispiel verwendet die Eingabedatei `MessageInsightsDataSource`Parameter, um nach einem Betreff zu filtern, der mit „Hello“ beginnt, Ergebnisse auszuschließen, die "noreply@example.com" enthalten FromEmailAddress, und um ein CSV-Format für die Ausgabedatei anzugeben:

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Hello*"
```

```
                ]
            },
            "Exclude": {
                "FromEmailAddress": [
                    "noreply@example.com"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

- In diesem Beispiel verwendet die Eingabedatei `MessageInsightsDataSource`Parameter, um nach einem Betreff zu filtern, der mit „Hello“ beginnt, mit einer FromEmailAddress „Information“ an Ziele gesendet wird, die auf „@example .com“ enden, Gmail als ISP verwendet, ein letztes Zustellungsereignis von „DELIVERY“, ein letztes Engagement-Ereignis, das entweder „OPEN“ oder „CLICK“ lautet, und ein für die Ausgabedatei angegebenes .json-Format:

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Hello*"
                ],
                "FromEmailAddress": [
                    "*information*"
                ],
                "Destination": [
                    "*@example.com"
                ],
                "Isp": [
                    "Gmail"
                ],
                "LastDeliveryEvent": [
                    "DELIVERY"
                ],
```

```
                "LastEngagementEvent": [
                    "OPEN", "CLICK"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "JSON"
    }
}
```

- In diesem Beispiel verwendet die Eingabedatei `MessageInsightsDataSource`Parameter, um nach Zielen zu filtern, die mit „@example1 .com“, „@example2 .com“ oder „@example3 .com“ enden, Nachrichten auszuschließen, die „SEND“ oder „DELIVERY“ LastDeliveryEvent entsprechen, und ein für die Ausgabedatei angegebenes CSV-Format:

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Destination": [
                    "*@example1.com",
                    "*@example2.com",
                    "*@example3.com"
                ]
            },
            "Exclude": {
                "LastDeliveryEvent": [
                    "SEND",
                    "DELIVERY"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

Weitere Informationen über Parameterwerte und zugehörige Datentypen finden Sie in `MessageInsightsDataSource` als ein Objekt des Typs `ExportDataSource` in der Referenz für Amazon-SES-API v2.

Verwaltung Ihrer Exportaufträge mit dem AWS CLI

Diese Beispiele veranschaulichen, wie Sie Ihre Exportaufträge verwalten können, indem Sie sie auflisten, Informationen dazu abrufen und sie stornieren. Verwenden Sie dazu die AWS CLI.

Um Ihre Exportaufträge aufzulisten mit dem AWS CLI

Sie können die `ListExportJobs`-Operation der Amazon SES API v2 verwenden, um Ihre Exportaufträge aufzuführen. Sie können diesen Vorgang von der aus aufrufen, AWS CLI wie in den folgenden Beispielen gezeigt.

- Führen Sie Ihre Exportaufträge auf:

```
aws --region us-east-1 sesv2 list-export-jobs --export-source-type=METRICS_DATA
```

```
aws --region us-east-1 sesv2 list-export-jobs --job-status=CREATED
```

```
aws --region us-east-1 sesv2 list-export-jobs --cli-input-json file://list-export-jobs-input.json
```

- Die Eingabedatei sieht in etwa wie folgt aus:

```
{
  "NextToken": "",
  "PageSize": 0,
  "ExportSourceType": "METRICS_DATA",
  "JobStatus": "CREATED"
}
```

Weitere Informationen zu Parameterwerten für die `ListExportJobs`-Operation finden Sie in der Referenz zu Amazon SES API v2.

Um Informationen über Ihren Exportauftrag zu erhalten, verwenden Sie den AWS CLI

Sie können die GetExportJob-Operation von Amazon SES API v2 verwenden, um Informationen zu Ihren Exportaufträge abzurufen. Sie können diesen Vorgang von der aus aufrufen, AWS CLI wie in den folgenden Beispielen gezeigt.

- Rufen Sie Informationen zu Ihrem Exportauftrag ab:

```
aws --region us-east-1 sesv2 get-export-job --job-id=<JobId>
```

```
aws --region us-east-1 sesv2 get-export-job --cli-input-json file://get-export-job-input.json
```

- Die Eingabedatei sieht in etwa wie folgt aus:

```
{
    "JobId": "e2220d6b-dce5-45f2-bf60-3287a465b732"
}
```

  Weitere Informationen zu Parameterwerten für die GetExportJob-Operation finden Sie in der Referenz zu Amazon SES API v2.

Um Ihren Exportauftrag abzubrechen, verwenden Sie den AWS CLI

Sie können die CancelExportJob-Operation von Amazon SES API v2 verwenden, um Ihren Exportauftrag abzubrechen. Sie können diesen Vorgang von der aus aufrufen, AWS CLI wie in den folgenden Beispielen gezeigt.

- Ihren Exportauftrag abbrechen:

```
aws --region us-east-1 sesv2 cancel-export-job --job-id=<JobId>
```

```
aws --region us-east-1 sesv2 cancel-export-job --cli-input-json file://cancel-export-job-input.json
```

- Die Eingabedatei sieht in etwa wie folgt aus:

```
{
    "JobId": "e2220d6b-dce5-45f2-bf60-3287a465b732"
}
```

Weitere Informationen zu Parameterwerten für die `CancelExportJob`-Operation finden Sie in der Referenz zu Amazon SES API v2.

Den vollständigen Ereignisverlauf einer Nachricht und die Antworten des Internetdienstanbieters mit dem AWS CLI

Die folgenden Beispiele veranschaulichen, wie Sie mithilfe der AWS CLI Details zum vollständigen Ereignisverlauf einer Nachricht und zu allen Antworten oder Diagnosecodes anzeigen, die vom Postfachanbieter zurückgegeben wurden. Dies sind die gleichen Daten, die in der Seitenleiste Informationen zur Nachricht verwendet werden, nachdem Sie das Optionsfeld einer Nachricht in der Tabelle Nachrichten im Virtual-Deliverability-Manager-Dashboard auswählen.

Um den Ereignisverlauf einer Nachricht und die Antworten des Internetdienstanbieters einzusehen, verwenden Sie den AWS CLI

Sie können die `GetMessageInsights`-Operation in Amazon SES API v2 verwenden, um Details einer gesendeten Nachricht anzuzeigen. Sie können diesen Vorgang von der aus aufrufen, AWS CLI wie im folgenden Beispiel gezeigt.

- Zeigen Sie die Nachrichtendetails zu einer gesendeten E-Mail an, die anhand ihrer Nachrichten-ID identifiziert wird:

```
aws --region us-east-1 sesv2 get-message-insights --message-id
 01000100001000dd-2a19190d-99d4-0000-9f00-deb5bbf2bfbe-000001
```

  Weitere Informationen zu Parameterwerten für die `GetMessageInsights`-Operation finden Sie in der Referenz zu Amazon SES API v2.

So werden die Dashboard-Metriken des virtuellen Zustellbarkeitsmanagers berechnet

Alle Karten zu Raten und alle Detailtabellen, die im Dashboard von Virtual Deliverability Manager angezeigt werden, berechnen Metriken für den Zeitraum, der im Bereich Vollständige Kontoübersicht eingegeben wurde.

Die im Dashboard angezeigten Prozentsätze der Metrikraten werden wie in der Tabelle beschrieben berechnet. Die letzten vier Spalten stellen Kriterien für die grundlegende Mathematik dar, die

zur Ableitung der angezeigten Metriken verwendet wird. Die Open rate (Öffnungsrate) wird beispielsweise folgendermaßen berechnet: die Gesamtzahl der geöffneten Nachrichten geteilt durch die Summe der zugestellten HTML-Nachrichten, die mit aktivierter Interaktionsnachverfolgung zugestellt werden. Sie spiegeln keine der Nachrichten wider, die Sie ohne Interaktionsnachverfolgung gesendet haben, und sind nicht HTML-codiert.

Rate in Prozent	Wie erfolgt die Berechnung	Mit aktivierter Interaktionsnachverfolgung	Außerdem mit mindestens einem verfolgten Link	Wird ISPs mit einem SES FBL geliefert	Ausgeschlossen, wenn auf Ihrer Unterdrückungsliste auf Kontoebene
Open rate (Öffnungsrate)	offen insgesamt/zugestellt insgesamt	✓			
Taktrate	Klick insgesamt/zugestellt insgesamt	✓	✓		
Complaint rate (Beschwerderate)	Beschwerde insgesamt/ zugestellt insgesamt			✓	✓
Delivery rate (Zustellungsrate)	zugestellt insgesamt/versendet insgesamt				
Rate der vorübergehenden Unzustellbarkeit	vorübergehende Unzustellbarkeit insgesamt/versendet insgesamt				✓
Rate der permanenten Unzustellbarkeit	permanente Unzustellbarkeit insgesamt/versendet insgesamt				✓

Rate in Prozent	Wie erfolgt die Berechnung	Mit aktivierter Interaktionsnachverfolgung	Außerdem mit mindestens einem verfolgten Link	Wird ISPs mit einem SES FBL geliefert	Ausgeschlossen, wenn auf Ihrer Unterdrückungsliste auf Kontoebene
Versandvolumen insgesamt	Rate in Prozent wird nicht angezeigt (alles, was gesendet wurde; immer 100 %)				

So werden die Differenzrate und die Volumensummen für alle Metriken berechnet:

- Differenz in Prozent – der Unterschied zwischen der Metriksumme im Vergleich zur vorherigen Metriksumme für den angegebenen Zeitraum. Wenn beispielsweise Letzte 7 Tage der angegebene Datumsbereich ist, Metrikrate der letzten 7 Tage – Metrikrate der vorherigen 7 Tage.
  - Die Differenz in Prozent für das gesamte Versandvolumen wird anders berechnet. Beispiel: (Versandvolumen der letzten 7 Tage – Versandvolumen der vorherigen 7 Tage)/Versandvolumen der vorherigen 7 Tage.
- Volumen – Gesamtzahl jeder Metrik.

> **Note**
>
> - In der Spalte Delivered (Zugestellt) in den Detailtabellen wird das direkt zugestellte Volumen ohne die Kriterien „Zugestellt“ angezeigt, die zur Berechnung der Öffnungs-, Klick- und Beschwerderaten verwendet wurden.
> - Der virtuellen Zustellbarkeitsmanager erfasst nur Metriken von E-Mails, die einen Empfänger haben. E-Mails mit mehreren Empfängern werden in keiner der Dashboard-Metriken des virtuellen Zustellbarkeitsmanagers berücksichtigt.

- In diesen Fällen sind Ihre Virtual Deliverability Manager-Metrikzahlen niedriger als die Anzahl Ihrer CloudWatch Amazon-Kennzahlen, da die CloudWatch Metriken E-Mails mit mehreren Empfängern umfassen.
- An den SES-Postfachsimulator gesendete E-Mails werden in keiner der Dashboard-Metriken des virtuellen Zustellbarkeitsmanagers berücksichtigt.
- E-Mails, die über das Konto eines stellvertretenden Absenders gesendet wurden (früher kontoübergreifender Versand), werden in keiner der Dashboard-Metriken von Virtual Deliverability Manager gezählt.

Important

Der Datenschutz von Apple Mail und seine Auswirkungen auf die Interaktionsraten: Als Ergebnis der Implementierung der Mail-Datenschutzfunktion (Mail Privacy Protection, MPP) für Apple-Geräte ab Version i ist die Zahl der Interaktionen gestiegenOS15, da MPP-Trigger geöffnet werden, wenn die Apple Mail-App gestartet wird, und nicht unbedingt, wenn ein Empfänger eine Nachricht öffnet and/or und klickt. Dies führt dazu, dass die Interaktionsdaten viel höher aussehen, als sie es normalerweise sind, und dies müssen E-Mail-Vermarkter bei der Überprüfung der Interaktion berücksichtigen. Es gibt mehrere andere Möglichkeiten, Interaktionen zu identifizieren, wie z. B. Webaktivitäten, app/portal Nutzung und auch die Verwendung von Proxydaten von Geräten, die nicht von Apple stammen, um eine aggregierte Metrik zu erstellen. Das Wichtigste, worauf Sie sich konzentrieren sollten, sind die Interaktionstrends, da diese darauf hinweisen können, ob ein Problem mit Ihrem E-Mail-Versand besteht. Weitere Informationen finden Sie unter Datenschutz von Apple Mail.

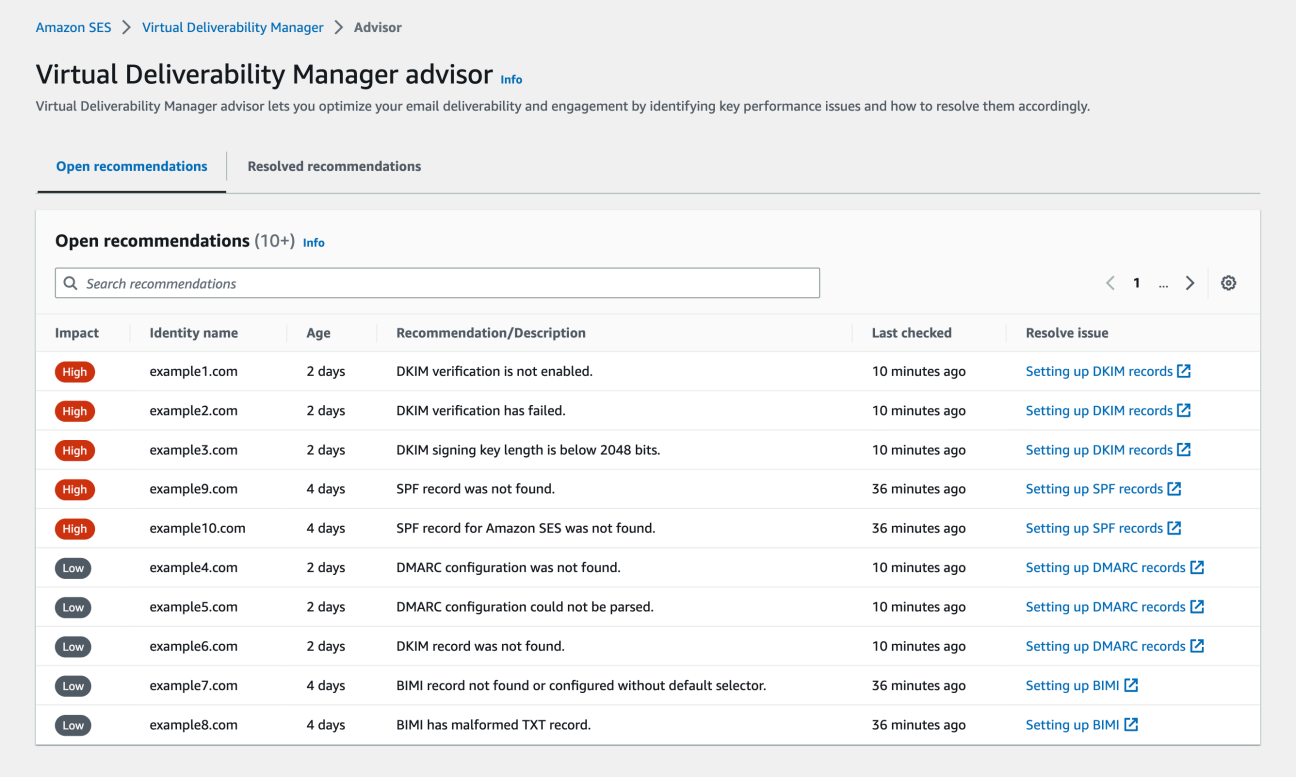
Berater für den virtuellen Zustellbarkeitsmanager

Der Berater für den virtuellen Zustellbarkeitsmanager hilft Ihnen dabei, die Zustellbarkeit und Interaktion für Ihre E-Mails zu optimieren, indem er wichtige Leistungs- und Infrastrukturprobleme auf Konto- und Sendeidentitätsebene identifiziert, die sich negativ auf Ihre E-Mail-Zustellbarkeit und Ihre Reputation auswirken. Er bietet Lösungen, indem er spezifische Anleitungen zur Behebung des identifizierten Problems bereitstellt.

Die Infrastrukturempfehlungen des Beraters sind in der Tabelle Open recommendations (Offene Empfehlungen) aufgeführt. Die Empfehlungen identifizieren Standardprobleme bei der E-Mail-Authentifizierung, z. B. wenn SPF-, DKIM-, DMARC- oder BIMI-Einträge nicht vorhanden sind

oder Probleme mit der Konfiguration auftreten, wie falsche Formatierung oder eine zu kurze Schlüssellänge. Sie werden nach dem Schweregrad von Impact (Auswirkungen), dem Identity name (Identitätsname) der sendenden Domain und dem Age (Alter) der Warnung kategorisiert. In der Suchleiste bietet ein Listenfeld die Möglichkeit, nach Auswirkungsgrad, Infrastrukturkategorie oder Namen der Sendeidentität zu filtern. In der Spalte Last checked (Zuletzt geprüft) wird der relative Zeitpunkt der letzten Aktualisierung der Empfehlung angezeigt, z. B. „Just now“ (Gerade) oder „15 minutes ago“ (Vor 15 Minuten). Die letzte Spalte, Resolve issue (Problem lösen), enthält einen Link zum entsprechenden Abschnitt im Amazon-SES-Entwicklerhandbuch mit Anleitungen zur Lösung des identifizierten Problems.

Offene Empfehlungen werden im Berater für den virtuellen Zustellbarkeitsmanager nach Wirkungsgrad sortiert angezeigt.



Wenn keine laufenden Berater-Benachrichtigungen vorhanden sind, erhalten Sie in einer Nachricht den Hinweis, dass keine offenen Empfehlungen vorliegen. Wir empfehlen Ihnen, den Berater regelmäßig zu überprüfen. Optional können Sie diese Advisor-Benachrichtigungsereignisse in Amazon integrieren EventBridge , um skalierbare, ereignisgesteuerte Anwendungen zu erstellen, wie unter beschrieben. Überwachung mit EventBridge

Auf der Seite des Beraters für den virtuellen Zustellbarkeitsmanager können Sie auch auf die Tabelle Resolved recommendations (Gelöste Empfehlungen) zugreifen, in der Infrastrukturprobleme

aufgeführt sind, die Sie durch die Umsetzung der Beraterempfehlungen gelöst haben. Behobene Empfehlungen werden mit einem Anfangsstatus aufgeführt, der das Problem beschreibt, bevor es behoben wurde. Gelöste Empfehlungen laufen nach 30 Tagen ab.

Wonach sucht der Berater von Virtual Deliverability Manager

Im vorherigen Abschnitt haben wir besprochen, dass der Berater von Virtual Deliverability Manager Prüfungen anhand Ihrer Absenderdomäne durchführt, um festzustellen, ob Sie eine sicher authentifizierte Infrastruktur konfiguriert haben, um sicherzustellen, dass Sie eine hohe E-Mail-Zustellrate und einen guten Ruf als Absender aufrechterhalten. Bevor Sie den Virtual Deliverability Manager-Advisor aktivieren, halten wir es für hilfreich, wenn Sie genau wissen, was der Berater überprüft und wonach er in diesen Prüfungen sucht.

Sie können diese Tabelle als Referenz verwenden, um die Konfiguration Ihrer Absenderdomain durchzugehen und alle Elemente zu korrigieren, die nicht den in dieser Tabelle aufgeführten Standards entsprechen, bevor sie zu Problemen werden, auf die Sie der Berater aufmerksam machen muss.

Art der Prüfung	Nachricht des Beraters	Warum alarmiert Sie der Berater	WEITERE INFORMATIONEN
Überprüfen Sie die Quote der Beschwerden	*ISP_name*Der ISP hat eine *high/med/low* Beschwerdequote.	Identity hat den Schwellenwert für Beschwerdeempfehlungen für diesen ISP überschritten.	Überwachen Ihrer Absenderzuverlässigkeit
DKIM-Konfiguration	Die DKIM-Überprüfung ist nicht aktiviert.	DKIM ist nicht pro Identität aktiviert.	Einfaches DKIM in SES
DKIM-Schlüsselstärke	Die Länge des DKIM-Signaturschlüssels liegt unter 2048 Bit.	Die Länge des DKIM-Signaturschlüssels verwendet nicht mindestens 2048 Bit.	Einfaches DKIM in SES
Validierung von DKIM-DNS-Einträgen	Die DKIM-Überprüfung ist fehlgeschlagen.	DKIM-CNAME-Einträge wurden nach dem Suchen	Überprüfung einer DKIM-Domänenidenti

Art der Prüfung	Nachricht des Beraters	Warum alarmiert Sie der Berater	WEITERE INFORMATIONEN
		und Überprüfen des Schlüssels für ungültig befunden.	tät bei Ihrem DNS-Anbieter
DMARC-Konfiguration	Die DMARC-Konfiguration wurde nicht gefunden.	DMARC-TXT-Datensätze fehlen.	Einrichtung der DMARC-Richtlinie für Ihre Domain
Überprüfung des Formats von DMARC-DNS-Einträgen	Die DMARC-Konfiguration konnte nicht analysiert werden.	Für DMARC-TXT-Einträge wurde ein ungültiges Format gefunden.	Einrichtung der DMARC-Richtlinie für Ihre Domain
Die DKIM-Konfiguration von DMARC	Der DKIM-Eintrag wurde nicht gefunden.	Es wurde kein DKIM-Eintrag gefunden, der den DMARC-Anforderungen entspricht.	Einhaltung von DMARC durch DKIM
Die DKIM-Konfiguration von DMARC	Der DKIM-Datensatz ist nicht abgestimmt.	Die in der DKIM-Signatur angegebene Domäne stimmt nicht mit der Domäne in der Absenderadresse überein.	Einhaltung von DMARC durch DKIM
SPF-Konfiguration	Der SPF-Eintrag wurde nicht gefunden.	Der SPF-TXT-Eintrag fehlt für die Custom MAIL FROM-Domäne.	Konfiguration Ihrer benutzerdefinierten MAIL FROM-Domäne
SPF „Include“ ist konfiguriert	Der SPF-Eintrag für Amazon SES wurde nicht gefunden.	`include:amazonses.com` fehlt im SPF-TXT-Eintrag.	Konfiguration Ihrer benutzerdefinierten MAIL FROM-Domäne

Art der Prüfung	Nachricht des Beraters	Warum alarmiert Sie der Berater	WEITERE INFORMATIONEN
SPF-Durchsetzung konfiguriert	Der Qualifier „SPF all“ fehlt.	`~all`fehlt im SPF-TXT-Datensatz.	Konfiguration Ihrer benutzerdefinierten MAIL FROM-Domäne
Validierung der SPF-Durchsetzung	Es wurde ein Problem mit der SPF-Konfiguration gefunden.	Versuche, den erforderlichen SPF MX-Eintrag innerhalb von 72 Stunden zu finden, schlugen fehl.	Status der Einrichtung der benutzerdefinierten MAIL FROM-Domäne
BIMI ist konfiguriert	Der BIMI-Datensatz wurde ohne Standardauswahl nicht gefunden oder konfiguriert.	BIMI-TXT-Datensätze fehlen oder es fehlt das Selector-Attribut.	BIMI einrichten
Validierung des BIMI-Formats	BIMI hat einen fehlerhaften TXT-Datensatz.	Es wurde festgestellt, dass der BIMI-TXT-Datensatz falsch konfiguriert ist, nachdem geprüft wurde, ob folgende Elemente vorhanden sind und ob das Format gültig ist: Version, Zertifikat-URL und Logo-URL.	BIMI einrichten

Verwenden des virtuellen Zustellbarkeitsmanagers in der Amazon-SES-Konsole

Das folgende Verfahren zeigt Ihnen, wie Sie den Berater für den virtuellen Zustellbarkeitsmanager in der Amazon-SES-Konsole verwenden, um identifizierte Zustellungsprobleme mit der Amazon-SES-Konsole zu lösen.

So verwenden Sie den Berater für den virtuellen Zustellbarkeitsmanager, um Probleme bei der Zustellbarkeit und der Reputation zu lösen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Virtual Deliverability Manager (Virtueller Zustellbarkeitsmanager) die Option Advisor (Berater) aus.

   > **Note**
   >
   > Der Advisor (Berater) wird nicht angezeigt, wenn Sie den virtuellen Zustellbarkeitsmanager nicht für Ihr Konto aktiviert haben. Weitere Informationen finden Sie unter the section called “Erste Schritte”.

3. Die Tabelle Open recommendations (Offene Empfehlungen) wird standardmäßig angezeigt. Empfehlungen werden nach Impact (Auswirkung) (Hoch/Niedrig), Identity name (Identitätsname) (Sendedomäne), Age (Alter) (der Warnung) und Recommendation/Description (Empfehlung/Beschreibung) (identifiziertes Problem) kategorisiert. Filtern Sie in der Suchleiste nach der Ebene der Impact (Auswirkung), der Category (Kategorie) des Infrastrukturproblems oder dem Identity name (Identitätsnamen) der Sendedomäne.
4. Wenn Sie ein Problem beheben möchten, das in der Spalte Recommendation/Description (Empfehlung/Beschreibung) beschrieben wird, wählen Sie den Link in der Spalte Resolve issue (Problem lösen) für diese Zeile aus und implementieren Sie die vorgeschlagene Lösung.

   > **Note**
   >
   > Nachdem Sie eine Lösung implementiert haben, kann es bis zu sechs Stunden dauern, bis das gelöste Problem behoben ist. Sie können das behobene Problem auf der Registerkarte Resolved recommendations (Behobene Empfehlungen) einsehen.

Zugriff auf Ihre Virtual Deliverability Manager-Empfehlungen über AWS CLI

Die folgenden Beispiele zeigen Ihnen, wie Sie mithilfe der AWS CLI auf die Empfehlungen des virtuellen Zustellbarkeitsmanagers zugreifen.

Um auf Ihre Virtual Deliverability Manager-Empfehlungen zuzugreifen, verwenden Sie den AWS CLI

Sie können den `ListRecommendations`-Vorgang in der Amazon-SES-API v2 verwenden, um Ihre Zustellbarkeitsempfehlungen aufzulisten. Sie können diese Operation von der AWS CLI aus aufrufen, wie in den folgenden Beispielen dargestellt.

- Listen Sie die Empfehlungen auf, um Probleme mit der Zustellbarkeit zu erkennen:

```
aws --region us-east-1 sesv2 list-recommendations
```

- Wenden Sie Filter an, um Empfehlungen für eine bestimmte Domäne in Ihrem Besitz abzurufen:

```
aws --region us-east-1 sesv2 list-recommendations --cli-input-json file://list-
recommendations.json
```

- Die Eingabedatei sieht in etwa wie folgt aus:

```
{
  "PageSize":100,
  "Filter":{
    "RESOURCE_ARN": "arn:aws:ses:us-east-1:123456789012:identity/example.com"
   }
}
```

Einstellungen des virtuellen Zustellbarkeitsmanagers

In Ihrem Konto können Sie die Einstellungen des virtuellen Zustellbarkeitsmanagers jederzeit einsehen oder ändern. Sie können Virtual Deliverability Manager aktivieren oder deaktivieren und auf Virtual Deliverability Manager-Kontoebene über die Amazon SES SES-Konsole oder die AWS CLI

Optionen des virtuellen Zustellbarkeitsmanagers werden auch auf der Ebene des Konfigurationssatzes bereitgestellt, damit Sie benutzerdefinierte Einstellungen dafür definieren können, wie ein Konfigurationssatz die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung verwendet, indem Sie die i, virtuellen Zustellbarkeitsmanager definierten Einstellungen

überschreiben. Damit erhalten Sie die Flexibilität, Ihren E-Mail-Versand an bestimmte E-Mail-Kampagnen anzupassen. Sie können beispielsweise die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung für Ihre Marketing-E-Mails aktivieren und für Ihre Transaktions-E-Mail deaktivieren.

Ändern der Einstellungen des Kontos des virtuellen Zustellbarkeitsmanagers mithilfe der Amazon-SES-Konsole

Die folgende Vorgehensweise zeigt Ihnen, wie Sie die Kontoeinstellungen vom virtuellen Zustellbarkeitsmanager mithilfe der Amazon-SES-Konsole ändern.

So ändern Sie die Einstellungen des Kontos des virtuellen Zustellbarkeitsmanagers mithilfe der Amazon-SES-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Virtual Deliverability Manager (Virtueller Zustellbarkeitsmanager) die Option Settings (Einstellungen) aus.

   Die Seite mit den Einstellungen des virtuellen Zustellbarkeitsmanagers wird geöffnet. Im Bereich Subscription overview (Abonnementübersicht) wird der Status des virtuellen Zustellbarkeitsmanagers angezeigt, und im Bereich Additional settings (Zusätzliche Einstellungen) wird der Status von Engagement Tracking (Interaktionsnachverfolgung) sowie Optimized Shared Delivery (Optimierte gemeinsame Zustellung) angezeigt.
3. So ändern Sie die Einstellungen für Engagement tracking (Interaktionsnachverfolgung) oder die Optimized shared delivery (Optimierte gemeinsame Zustellung):

   a. Wählen Sie im Bereich Additional settings (Zusätzliche Einstellungen) die Option Edit (Bearbeiten) aus.

   b. Wählen Sie das entsprechende Optionsfeld aus, um eine der Funktionen ein- oder auszuschalten, und wählen Sie dann Submit settings (Einstellungen senden) aus.

      Auf der Seite Virtual Deliverability Manager settings (Einstellungen für virtuellen Zustellbarkeitsmanager) wird im Bereich Additional settings (Zusätzliche Einstellungen) eine Zusammenfassung Ihrer Änderungen angezeigt.

> **Note**
>
> Die Optionen für die Interaktionsnachverfolgung, die Sie hier oder in Konfigurationssatz-Überschreibungen für den virtuellen Zustellbarkeitsmanager definieren, legen fest, ob Öffnungs- und Klickereignisse im Dashboard des virtuellen Zustellbarkeitsmanagers angezeigt werden. Sie wirken sich nicht auf Ereigniszielkonfigurationen aus, die Öffnungs- und Klickereignisse veröffentlichen. Wenn Sie beispielsweise die Interaktionsnachverfolgung hier deaktiviert haben, wird die Ereignisveröffentlichung für Öffnungs- und Klickereignisse, die Sie in den SES-Ereigniszielen eingerichtet haben, nicht deaktiviert.

4. (Optional) Damit Sie benutzerdefinierte Einstellungen dafür definieren können, wie ein Konfigurationssatz die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung verwendet, indem Sie die im virtuellen Zustellbarkeitsmanager definierten Einstellungen überschreiben, sehen Sie sich bei Bearbeitung oder Änderung eines Konfigurationssatzes die Optionen für virtuellen Zustellbarkeitsmanager an.
5. So deaktivieren Sie den virtuellen Zustellbarkeitsmanager:
   a. Wählen Sie im Bereich Subscription overview (Abonnementübersicht) die Option Disable Virtual Deliverability Manager (Virtuellen Zustellbarkeitsmanager deaktivieren) aus.
   b. Geben Sie im Popup-Fenster Disable Virtual Deliverability Manager? (Virtuellen Zustellbarkeitsmanager deaktivieren?) im Bestätigungsfeld `Disable` ein und wählen Sie dann Disable Virtual Deliverability Manager (Virtuellen Zustellbarkeitsmanager deaktivieren) aus.
   c. Ein Banner wird angezeigt, in dem bestätigt wird, dass Sie den virtuellen Zustellbarkeitsmanager deaktiviert haben.
6. Informationen zur erneuten Aktivierung des virtuellen Zustellbarkeitsmanagers finden Sie unter the section called “Erste Schritte”.

Ändern Sie Ihre Virtual Deliverability Manager-Kontoeinstellungen mithilfe der AWS CLI

Sie können die Einstellungen des Kontos des virtuellen Zustellbarkeitsmanagers mithilfe der AWS CLIändern.

Um Ihre Virtual Deliverability Manager-Kontoeinstellungen zu ändern, verwenden Sie AWS CLI

Mit den Operationen `PutAccountVdmAttributes` und `PutConfigurationSetVdmOptions` in der Amazon-SES-API v2 können Sie die Einstellungen des virtuellen Zustellbarkeitsmanagers ändern. Sie können diesen Vorgang von der aus aufrufen AWS CLI, wie in den folgenden Beispielen gezeigt.

- Aktivieren oder deaktivieren Sie die Interaktionsnachverfolgung, die optimierte gemeinsame Zustellung oder beides mithilfe einer Eingabedatei:

  ```
  aws --region us-east-1 sesv2 put-account-vdm-attributes --cli-input-json file://
  attributes.json
  ```

  In diesem Beispiel, in dem die Interaktionsnachverfolgung `ENABLED` und die optimierte gemeinsame Zustellung `DISABLED` ist, sieht die Eingabedatei etwa wie folgt aus:

  ```
  {
      "VdmAttributes": {
          "VdmEnabled": "ENABLED",
          "DashboardAttributes": {
              "EngagementMetrics": "ENABLED"
          },
          "GuardianAttributes": {
              "OptimizedSharedDelivery": "DISABLED"
          }
      }
  }
  ```

  Sie finden weitere Informationen über Parameterwerte und zugehörige Datentypen durch eine Verknüpfung mit dem `VdmAttributes`-Datentyp in der Referenz für Amazon-SES-API v2.

- Definieren Sie benutzerdefinierte Einstellungen dafür, wie ein Konfigurationssatz die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung nutzt, indem die im virtuellen Zustellbarkeitsmanager definierten Einstellungen außer Kraft gesetzt werden:

  ```
  aws --region us-east-1 sesv2 put-configuration-set-vdm-options --cli-input-json
   file://config-set.json
  ```

  In diesem Beispiel, in dem ein Konfigurationssatz namens Beispiel die Interaktionsnachverfolgung und die optimierte gemeinsame Zustellung aktiviert ist, ähnelt die Eingabedatei wie folgt aus:

```
{
    "ConfigurationSetName": "example",
    "VdmOptions": {
        "DashboardOptions": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianOptions": {
            "OptimizedSharedDelivery": "ENABLED"
        }
    }
}
```

Weitere Informationen über Parameterwerte und zugehörige Datentypen finden Sie im `VdmOptions`-Datentyp in der Referenz für Amazon-SES-API v2.

- So überprüfen Sie das Ergebnis:

```
aws –region us-east-1 sesv2 get-configuration-set –configuration-set-name example
```

- Wenn Sie auf der Ebene des Konfigurationssatzes die Optionen `DashboardOptions` oder `GuardianOptions` nicht angeben, gelten Ihre Kontoeinstellungen des virtuellen Zustellbarkeitsmanagers für den Datenverkehr, der über diesen Konfigurationssatz gesendet wird.

E-Mail-Validierung für Amazon SES

Die Qualität der E-Mail-Listen ist ein entscheidender Faktor für die Aufrechterhaltung hoher Zustellungsraten und den Schutz Ihres Rufs als Absender. Ungültige oder riskante E-Mail-Adressen können zu hohen Absprungraten und Spam-Beschwerden führen. Postfachanbieter können E-Mails ablehnen, Absenderdomänen auf eine schwarze Liste setzen oder die Zustellungsraten drosseln.

Die E-Mail-Validierung ist eine Amazon SES SES-Funktion, mit der Sie E-Mail-Adressen überprüfen können, bevor Sie sie an sie senden. Sie überprüft E-Mail-Adressen auf Syntaxfehler, die Domaingültigkeit und andere Prüfungen und identifiziert riskante Adressen, die Ihrem Ruf als Absender schaden könnten. So können Sie hohe Zustellraten aufrechterhalten und Ihren Ruf als Absender schützen.

Warum sind Qualität und Validierung von E-Mail-Listen wichtig?

Postfachanbieter überwachen wichtige Kennzahlen wie Absprungraten, Beschwerdequoten und Interaktionsgrad, um die Reputation der Absender zu bewerten. Wenn diese Kennzahlen akzeptable Schwellenwerte überschreiten, ergreifen die Anbieter Schutzmaßnahmen wie Ratenbegrenzung, vorübergehende Stundungen oder permanente Sperren. Hohe Absprungraten (in der Regel über 5 bis 10%) deuten auf eine schlechte Listenhygiene hin und führen zu sofortigen Reputationsstrafen.

Postfachanbieter erwarten von den Absendern, dass sie saubere E-Mail-Listen führen und gute Versandpraktiken nachweisen. Sie verfolgen Hard-Bounces von ungültigen Adressen, überwachen Spam-Trap-Treffer und messen das Engagement der Empfänger, um die Platzierung im Posteingang zu bestimmen. Eine schlechte Listenqualität hat messbare Auswirkungen: geringere Zustellungsraten, erhöhte Latenz und potenzielle Blacklists, die sich auf alle future Kampagnen von Ihrer Absenderdomain oder IP-Adresse aus auswirken.

Wie kann die E-Mail-Validierung dazu beitragen, die Zustellbarkeit und den Ruf zu verbessern?

Mit der E-Mail-Validierung können Sie sowohl Ihre Zustellbarkeit als auch Ihren Ruf verbessern. Dazu gehören eine API, die E-Mail-Adressen bei Bedarf überprüft, und die automatische Validierung, die ausgehende E-Mails anhand der von Ihnen festgelegten Schwellenwerte für die Zustellbarkeit automatisch überprüft und filtert.

- API-Validierung — Validiert E-Mail-Adressen mithilfe von API-Aufrufen, sodass Sie Adressen bereits bei der Erfassung überprüfen können, z. B. bei Anmeldeformularen oder Abonnementvorgängen, sowie bei der regelmäßigen Listenbereinigung vorhandener Datenbanken. Auf diese Weise wird verhindert, dass ungültige Adressen in Ihre Datenbank gelangen,

gibt Benutzern zeitnahes Feedback zur Adressgültigkeit und ermöglicht die regelmäßige Aufrechterhaltung der Qualität der E-Mail-Listen.

- Automatische Überprüfung — Überprüft automatisch alle ausgehenden E-Mail-Adressen und stellt nur Nachrichten an Empfänger zu, die den von Ihnen ausgewählten Schwellenwert für die Zustellungswahrscheinlichkeit (hoch oder mittel) erreichen. Dadurch wird Ihr Ruf als Absender geschützt, indem das Senden an ungültige oder riskante Adressen verhindert wird, ohne dass manuelles Eingreifen erforderlich ist.

Topics

- E-Mail-Validierungs-API
- Automatische Validierung
- E-Mail-Validierungs-Dashboard

E-Mail-Validierungs-API

Die API-Validierung ermöglicht es Ihnen, einzelne E-Mail-Adressen durch API-Aufrufe zu validieren und so sofort Feedback zur Adressgültigkeit, Zustellbarkeit und Risikofaktoren zu erhalten. Diese Funktion wurde für die Überprüfung von Adressen zum Zeitpunkt der Erfassung entwickelt, z. B. bei der Benutzerregistrierung, bei Abonnementformularen oder in jedem anderen Szenario, in dem Sie zeitnahe Überprüfungsergebnisse benötigen.

Bei der API-Validierung werden für jede E-Mail-Adresse mehrere Prüfungen durchgeführt, darunter Syntaxvalidierung, Domainüberprüfung, Überprüfung der Existenz von Postfächern und andere. Zu den Validierungsergebnissen gehören Vertrauensurteile (HOCH, MITTEL oder NIEDRIG) für die Gesamtvalidität und individuelle Bewertungen.

Validierungsprüfungen wurden durchgeführt

Bei der API-Validierung werden für jede E-Mail-Adresse die folgenden Bewertungen durchgeführt:

- Syntaxvalidierung (HasValidSyntax") — Überprüft, ob die E-Mail-Adresse den richtigen RFC-Standards entspricht und gültige Zeichen im richtigen Format enthält.
- DNS-Einträge ('HasValidDnsRecords') — Überprüft, ob die Domain existiert, gültige DNS-Einträge hat und für den Empfang von E-Mails konfiguriert ist.
- Existenz des Postfachs (MailboxExists") — Überprüft, ob das Postfach existiert und Nachrichten empfangen kann, ohne tatsächlich eine E-Mail zu senden.

- Rollenadresse ('IsRoleAddress') — Identifiziert rollenbasierte Adressen (wie admin@, support@ oder info@), die möglicherweise niedrigere Interaktionsraten aufweisen.
- Einwegdomäne ('IsDisposable') — Überprüft verfügbare oder temporäre E-Mail-Adressen, die sich negativ auf Ihren Ruf als Absender auswirken könnten.
- Zufällige Zeichenkettenmuster (IsRandomInput") — Überprüft zufällig generierte Muster.

API-Validierung mit der Amazon SES SES-Konsole verwenden

Das folgende Verfahren zeigt Ihnen, wie Sie eine E-Mail-Adresse mithilfe der Amazon SES SES-Konsole validieren.

Um eine E-Mail-Adresse mit der Amazon SES SES-Konsole zu validieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter E-Mail-Validierung die Option Überprüfung von E-Mail-Adressen aus.
3. Geben Sie im Abschnitt E-Mail-Adresse validieren die E-Mail-Adresse, die Sie validieren möchten, in das Feld E-Mail-Adresse ein.
4. Wählen Sie Validieren aus.

   Die Überprüfungsergebnisse werden im Fenster mit den Überprüfungsergebnissen angezeigt und zeigen:

   - IsValid— Gesamtvalidität mit einem Vertrauensurteil (HOCH, MITTEL oder NIEDRIG).
   - Bewertungen — Individuelle Bewertungsergebnisse mit Vertrauensurteilen zur Syntax, zu DNS-Einträgen, zum Vorhandensein von Postfächern und zu den oben aufgeführten Risikofaktoren.

Verwenden der API-Validierung mit dem AWS CLI

Die folgenden Beispiele zeigen Ihnen, wie Sie E-Mail-Adressen mit dem validieren AWS CLI.

Um eine E-Mail-Adresse mit dem zu validieren AWS CLI

Sie können den GetEmailAddressInsightsVorgang in der Amazon SES API v2 verwenden, um E-Mail-Adressen zu validieren. Sie können diesen Vorgang von der aus aufrufen AWS CLI, wie in den folgenden Beispielen gezeigt.

- Bestätigen Sie eine einzelne E-Mail-Adresse:

```
aws --region us-east-1 sesv2 get-email-address-insights --email-address
 user@example.com
```

- Die Antwort sieht in etwa wie folgt aus:

```
{
    "MailboxValidation": {
        "IsValid": {
            "ConfidenceVerdict": "HIGH"
        },
        "Evaluations": {
            "HasValidSyntax": {
                "ConfidenceVerdict": "HIGH"
            },
            "HasValidDnsRecords": {
                "ConfidenceVerdict": "MEDIUM"
            },
            "MailboxExists": {
                "ConfidenceVerdict": "MEDIUM"
            },
            "IsRoleAddress": {
                "ConfidenceVerdict": "LOW"
            },
            "IsDisposable": {
                "ConfidenceVerdict": "LOW"
            },
            "IsRandomInput": {
                "ConfidenceVerdict": "LOW"
            }
        }
    }
}
```

- Weitere Informationen zu Antwortwerten und Datentypen finden Sie unter dem MailboxValidationDatentyp in der Amazon SES API v2-Referenz.

- Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen für API-Aufrufe und die Veröffentlichung von CloudWatch Kennzahlen für die E-Mail-Validierung verfügt:

```
{
  "Version": "2012-10-17       ",
  "Statement": [
    {
      "Sid": "EmailValidationPermissions",
      "Effect": "Allow",
      "Action": [
        "ses:GetEmailAddressInsights",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

  Die `GetEmailAddressInsights` Genehmigung ist für API-Validierungsaufrufe erforderlich und `CreateServiceLinkedRole` ermöglicht die Veröffentlichung von CloudWatch Metriken für Validierungsaktivitäten.

Interpretation der Validierungsergebnisse

Die Antwort auf die Validierung enthält Vertrauensurteile, die Ihnen helfen sollen, Entscheidungen über E-Mail-Adressen zu treffen:

- `IsValid`— Bewertung der Gesamtvalidität mit einem Vertrauensurteil von HOCH, MITTEL oder NIEDRIG. Eine HOHE Validitätssicherheit bedeutet eine hohe Zustellungswahrscheinlichkeit für die E-Mail-Adresse, MITTEL steht für eine mäßige Zustellungswahrscheinlichkeit und NIEDRIG für eine niedrige Zustellungswahrscheinlichkeit.
- `Evaluations`— Individuelle Bewertungsergebnisse, jeweils mit einem Vertrauensurteil:
  - `HIGH`— Deutlicher Hinweis auf den spezifischen Scheck (z. B. HOCH für IsRandomInput bedeutet, dass die E-Mail sehr wahrscheinlich zufällig generiert wurde).
  - `MEDIUM`— Moderate Angabe des spezifischen Schecks (z. B. MEDIUM für IsRandomInput bedeutet, dass eine gewisse Wahrscheinlichkeit besteht, dass die E-Mail-Adresse zufällig generiert wurde).

- `LOW`— Schwacher oder kein Hinweis auf den spezifischen Scheck (z. B. „NIEDRIG“ IsRandomInput bedeutet, dass die E-Mail-Adresse weniger wahrscheinlich zufällig generiert wurde).

Automatische Validierung

Die automatische Validierung überprüft vor dem Senden automatisch alle ausgehenden E-Mail-Adressen und übermittelt nur Nachrichten an Empfänger, die den von Ihnen ausgewählten Bestätigungsschwellenwert erreichen. Auf diese Weise können Sie Ihren Ruf als Absender schützen, indem Sie verhindern, dass E-Mails an wahrscheinlich ungültige oder riskante Adressen gesendet werden, ohne dass manuelles Eingreifen oder API-Integration erforderlich sind.

Wenn die automatische Validierung aktiviert ist, validiert Amazon SES jede Empfängeradresse im Rahmen des Zustellversuchs. Adressen, die Ihren Schwellenwert nicht erreichen, werden automatisch unterdrückt. Sie können auch per Konfiguration festgelegte Ereignisziele einrichten, um nachzuverfolgen, welche E-Mails den Gültigkeitsschwellenwert nicht überschritten haben.

Schwellenwerte für die Validierung

Auto Validation unterstützt derzeit drei Validierungsschwellenwerte:

- SES verwaltet — Amazon SES verwaltet automatisch den Schwellenwert zur Unterdrückung ungültiger Adressen. Mit dieser Option kann Amazon SES den Validierungsschwellenwert auf der Grundlage Ihrer Versandmuster und Ihres Rufs optimieren.
- Hoch — Ermöglicht den Versand von E-Mails nur an Adressen mit hoher Zustellungswahrscheinlichkeit. Dies bietet maximalen Schutz für Ihren Ruf als Absender, kann jedoch dazu führen, dass einige legitime Adressen mit mittlerer Zustellungssicherheit unterdrückt werden.
- Mittel — Ermöglicht den Versand von E-Mails an Adressen mit mittlerer oder hoher Zustellungswahrscheinlichkeit. Auf diese Weise wird ein ausgewogenes Verhältnis zwischen Reputationsschutz und Zustellungsreichweite hergestellt, indem Adressen mit mittlerer und hoher Zustellungssicherheit zugelassen werden. Dadurch wird die Zustellung an E-Mail-Adressen mit geringer Zustellungssicherheit unterdrückt.

> **Important**
>
> Wenn Sie sich für hohe oder mittlere Schwellenwerte anstelle von SES Managed entscheiden, ist es wichtig, dass Sie Ihre Lieferkennzahlen und Validierungsergebnisse regelmäßig überprüfen.

Verwaltung der automatischen Validierung mit der Amazon SES SES-Konsole

Das folgende Verfahren zeigt Ihnen, wie Sie die Einstellungen für die automatische Validierung mithilfe der Amazon SES SES-Konsole aktivieren oder ändern können.

So verwalten Sie die automatische Validierung mit der Amazon SES SES-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter E-Mail-Validierung die Option Automatische Validierung aus.
3. Wählen Sie das Kontrollkästchen Aktiviert aus, um die Funktion zu aktivieren.
4. Wählen Sie einen Validierungsschwellenwert.
5. Wählen Sie Änderungen speichern aus.

   Im Bereich Automatische Validierung werden Ihre aktualisierten Einstellungen angezeigt.

> **Important**
>
> Die automatische Validierung gilt für alle ausgehenden E-Mails, die über Ihr Konto gesendet werden. Adressen, die Ihren Schwellenwert nicht erreichen, werden unterdrückt. Sie haben auch die Möglichkeit, die auto Validierung auf der Ebene des Konfigurationssatzes zu aktivieren. Unterdrückte Sendungen werden weiterhin auf Ihr tägliches Versandkontingent angerechnet und Ihnen wird zusätzlich zur Gebühr für die auto Überprüfung weiterhin die Standardgebühr für ausgehende Nachrichten für unterdrückte Sendungen berechnet. Informationen zur Preisgestaltung finden Sie auf der Seite SES – Preise.

Aktivieren Sie die automatische Validierung auf der Ebene des Konfigurationssatzes

Sie können die Einstellungen für die automatische Überprüfung auf Kontoebene für bestimmte Konfigurationssätze überschreiben. Auf diese Weise können Sie unterschiedliche Validierungsschwellenwerte für verschiedene Arten von E-Mail-Kampagnen anwenden.

Um die automatische Validierung für einen Konfigurationssatz zu konfigurieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Konfiguration die Option Konfigurationssätze aus.
3. Wählen Sie den Konfigurationssatz aus, den Sie konfigurieren möchten.
4. Wählen Sie im Abschnitt Optionen für die automatische Überprüfung die Option Bearbeiten aus.
5. Aktivieren Sie das Kontrollkästchen Einstellungen für die automatische Überprüfung auf Kontoebene außer Kraft setzen.
6. Aktivieren Sie das Kontrollkästchen Automatische Validierung aktiviert, um die automatische Validierung für diesen Konfigurationssatz zu aktivieren.
7. Wählen Sie für den Schwellenwert für die Validierung eine der folgenden Optionen aus:
   - SES-verwaltet — Amazon SES verwaltet den Schwellenwert automatisch.
   - Hoch — Nur Adressen mit hoher Lieferwahrscheinlichkeit.
   - Mittel — Adressen mit mittlerer Zustellungswahrscheinlichkeit.
8. Wählen Sie Änderungen speichern aus.

Wenn Sie die Einstellungen auf Kontoebene nicht überschreiben, verwendet der Konfigurationssatz die auf Kontoebene definierten Einstellungen für die automatische Validierung. Sie können auch Veranstaltungsziele einrichten, um nachzuverfolgen, welche E-Mails den Gültigkeitsschwellenwert nicht überschritten haben.

Verwaltung der automatischen Validierung mit dem AWS CLI

Die folgenden Beispiele zeigen Ihnen, wie Sie die automatische Validierung mithilfe von aktivieren und konfigurieren AWS CLI.

Um die automatische Validierung mit dem zu verwalten AWS CLI

Sie können den PutAccountSuppressionAttributesVorgang in der Amazon SES API v2 verwenden, um die automatische Validierung zu verwalten. Sie können diesen Vorgang von der aus aufrufen AWS CLI, wie in den folgenden Beispielen gezeigt.

- Aktivieren Sie die automatische Validierung mit einem hohen Schwellenwert:

```
aws --region us-east-1 sesv2 put-account-suppression-attributes --cli-input-json
 file://auto-validation.json
```

  Die Eingabedatei sieht in etwa wie folgt aus:

```
{
    "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
    "ValidationOptions": {
        "ConditionThreshold": {
            "ConditionThresholdEnabled": "ENABLED",
            "OverallConfidenceThreshold": {
                "Verdict": "HIGH"
            }
        }
    }
}
```

- Ändern Sie den Schwellenwert auf mittel:

```
{
    "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
    "ValidationOptions": {
        "ConditionThreshold": {
            "ConditionThresholdEnabled": "ENABLED",
            "OverallConfidenceThreshold": {
                "Verdict": "MEDIUM"
            }
        }
    }
}
```

- Verwenden Sie den von SES verwalteten Schwellenwert:

```
{
    "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
    "ValidationOptions": {
```

```
        "ConditionThreshold": {
            "ConditionThresholdEnabled": "ENABLED",
            "OverallConfidenceThreshold": {
                "Verdict": "MANAGED"
            }
        }
    }
}
```

- Automatische Validierung deaktivieren:

```
{
    "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
    "ValidationOptions": {
        "ConditionThreshold": {
            "ConditionThresholdEnabled": "DISABLED"
        }
    }
}
```

- So überprüfen Sie das Ergebnis:

```
aws --region us-east-1 sesv2 get-account
```

Weitere Informationen zu Parameterwerten und Datentypen finden Sie unter dem SuppressionAttributesDatentyp in der Amazon SES API v2-Referenz.

Um die automatische Validierung für einen Konfigurationssatz zu konfigurieren, verwenden Sie den AWS CLI

Sie können den PutConfigurationSetSuppressionOptionsVorgang verwenden, um die Einstellungen für die automatische Überprüfung für einen bestimmten Konfigurationssatz zu überschreiben.

- Einstellungen auf Kontoebene für einen Konfigurationssatz außer Kraft setzen:

```
aws --region us-east-1 sesv2 put-configuration-set-suppression-options --cli-input-
json file://config-set-auto-validation.json
```

Die Eingabedatei sieht in etwa wie folgt aus:

```
{
    "ConfigurationSetName": "my-config-set",
    "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
    "ValidationOptions": {
        "ConditionThreshold": {
            "ConditionThresholdEnabled": "ENABLED",
            "OverallConfidenceThreshold": {
                "Verdict": "HIGH"
            }
        }
    }
}
```

- So überprüfen Sie das Ergebnis:

```
aws --region us-east-1 sesv2 get-configuration-set --configuration-set-name my-
config-set
```

E-Mail-Validierungs-Dashboard

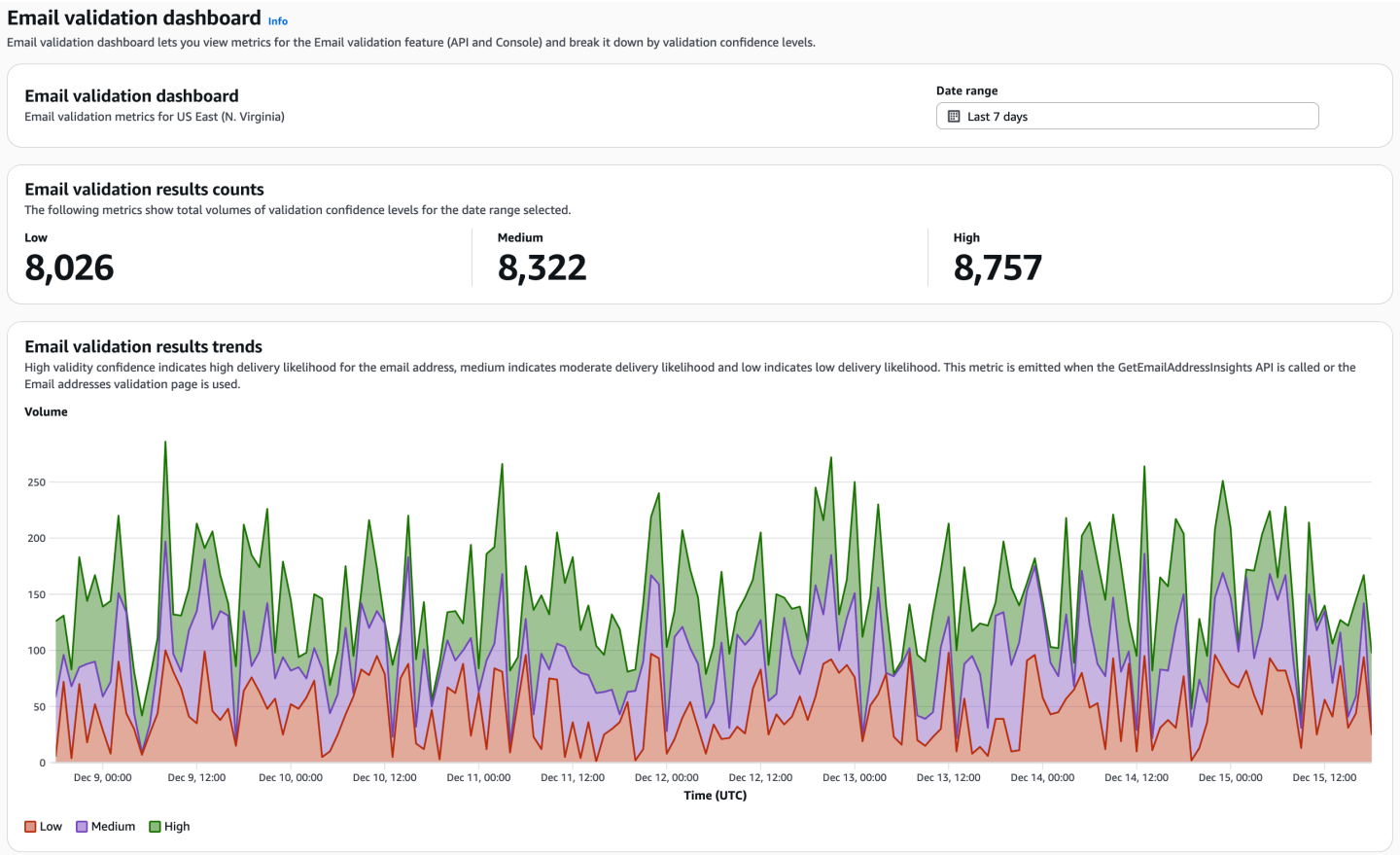
Das E-Mail-Validierungs-Dashboard bietet Einblick in Ihre E-Mail-Validierungsaktivitäten und zeigt die Validierungsergebnisse an, die nach Vertrauensstufen mit der Zustellungswahrscheinlichkeit kategorisiert sind. Sie können die Validierungstrends für API-Validierungen und Konsolenvalidierungen überwachen, um die Qualität Ihrer E-Mail-Listen zu verstehen und fundierte Entscheidungen über Ihre Versandpraktiken zu treffen.

Zugriff auf das Dashboard

So rufen Sie das E-Mail-Validierungs-Dashboard auf:

1. Melden Sie sich bei der Amazon SES SES-Konsole unter an https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich die Option E-Mail-Validierung aus.
3. Wählen Sie den Menüpunkt E-Mail-Validierungs-Dashboard, um die Validierungsmetriken anzuzeigen.

Das Dashboard bietet eine visuelle Darstellung Ihrer Validierungsaktivitäten und hilft Ihnen dabei, Trends zu erkennen und datengestützte Entscheidungen zu Listenhygiene und Versandpraktiken zu treffen.



Mail Manager für Amazon SES

Mail Manager ist eine Reihe von Amazon SES E-Mail-Gateway-Funktionen, mit denen Sie die E-Mail-Infrastruktur Ihres Unternehmens stärken, das E-Mail-Workflow-Management vereinfachen und die E-Mail-Compliance-Kontrolle optimieren können. Es lässt sich in Ihre bestehende Infrastruktur integrieren, kann verschiedene Geschäftsanwendungen verbinden und automatisiert die Verarbeitung eingehender E-Mails. Mail Manager fungiert auch als erste Verteidigungslinie bei der Aufrechterhaltung eines funktionierenden E-Mail-Systems, indem es Ihren E-Mail-Verkehr effizient verwaltet und die E-Mail-Archivierungsfunktionen für die Einhaltung von Vorschriften verbessert.

Neben den aktuellen Funktionen von Amazon SES umfasst Mail Manager die folgenden Funktionen, die eingehenden Datenverkehr unterstützen:

- Eingangsendpunkt — Eine wichtige Infrastrukturkomponente, die mithilfe von Filterrichtlinien und -regeln, die Sie konfigurieren können, bestimmt, welche E-Mails in Ihr Unternehmen gelangen dürfen und welche abgelehnt werden sollen.
- Richtlinien und Regelsätze für den Datenverkehr — Ermöglichen Sie E-Mail-Administratoren die Definition und Durchsetzung von Regeln für die Verwaltung des eingehenden E-Mail-Verkehrs mit hochgradig anpassbaren Richtlinien und Regeln, mit denen Sie E-Mails auf der Grundlage einer Vielzahl von von Ihnen definierten Bedingungen und Ausnahmen sortieren, kategorisieren, priorisieren und Aktionen für E-Mails ausführen können. Diese intelligente Filterung in Kombination mit automatisierten Workflows trägt dazu bei, die E-Mail-Verwaltung zu optimieren, die Effizienz zu steigern und die Einhaltung der E-Mail-Richtlinien Ihres Unternehmens sicherzustellen.
- SMTP-Relay — Leitet den E-Mail-Verkehr auf der Grundlage von Kriterien, die Sie in Regeln definieren, durch die Verbindung interner E-Mail-Systeme an andere SMTP-Server weiter und optimiert die E-Mail-Verwaltung durch automatische Weiterleitung. Durch die Möglichkeit, den Datenverkehr auf mehrere Server und Gateways zu verteilen, kann Ihr Unternehmen hohen E-Mail-Verkehr selbst in hybriden Umgebungen effektiv verwalten.
- E-Mail-Archivierung — Speichert und schützt Ihre E-Mails, indem Daten in einem dauerhaften und sicheren Langzeitspeicher gespeichert werden, und bietet Ihnen die Möglichkeit, E-Mails schnell zu suchen und zu archivieren. Es ermöglicht eine Vollzeitarchivierung auf Unternehmensebene, ohne die Speicheranforderungen Ihres Postfachservers zu erhöhen.
- E-Mail-Add-Ons — Eine Sammlung spezialisierter Sicherheitstools von von von SES zugelassenen Anbietern, mit denen Sie E-Mails verwalten können, die an Ihren Eingangsendpunkt gelangen, und mit denen Routing-Optionen auf der Grundlage von Sicherheitsergebnissen bereitgestellt werden können. Bei diesen Tools handelt es sich um zertifizierte Lösungen für Sicherheitsinformationen

und -durchsetzung, die sofort in Ihren E-Mail-Workflow integriert werden können und direkt von der Mail Manager-Konsole aus aktiviert werden können.

Erste Schritte mit Mail Manager

Um mit der Nutzung von Mail Manager zu beginnen, führt Sie ein Onboarding-Assistent in der Amazon SES SES-Konsole durch die Schritte zur Aktivierung von Mail Manager für Ihr Konto. Siehe the section called “Erste Schritte”.

Topics

- Erste Schritte mit Mail Manager
- Eingangsendpunkte
- Verkehrspolitik und Grundsatzerklärungen
- Regelsätze und Regeln
- SMTP-Relay
- Adresslisten
- E-Mail-Archivierung
- E-Mail-Add-Ons
- Berechtigungsrichtlinien für Mail Manager
- Mail Manager-Protokollierung

Erste Schritte mit Mail Manager

Um mit der Nutzung von Amazon SES Mail Manager zu beginnen, können Sie den Assistenten Erste Schritte mit Mail Manager in der Amazon SES SES-Konsole verwenden, wo Sie einen Eingangsendpunkt erstellen und ihn mit einer Datenverkehrsrichtlinie und einem Regelsatz konfigurieren.

Ein Eingangsendpunkt ist Ihr erster Baustein bei der Einrichtung von Mail Manager. Er ist eine wichtige Infrastrukturkomponente, die Folgendes nutzt:

- Verkehrsrichtlinien — Eine Verkehrsrichtlinie enthält Richtlinienerklärungen, die Sie definieren, um eingehende E-Mails zu sortieren, indem sie bestimmte Arten von E-Mails zulassen oder blockieren, wenn die Bedingungen der Richtlinienerklärung erfüllt sind.

- Regelsätze — Ein Regelsatz enthält Regeln, die Sie für die Ausführung von Aktionen mit der E-Mail definieren, die Sie zulassen, wenn die Bedingungen der Regel erfüllt sind.

Ein Teil der Erstellung eines Eingangsendpunkts besteht jedoch darin, eine Verkehrsrichtlinie und einen Regelsatz auszuwählen, die bereits erstellt wurden, und diese dann dem Eingangsendpunkt zuzuweisen. Die Schritte im folgenden Verfahren führen Sie durch die richtige Reihenfolge der Konfiguration Ihres ersten Eingangsendpunkts.

Erste Schritte mit Mail Manager mithilfe der SES-Konsole

Das folgende Verfahren zeigt Ihnen, wie Sie mit Mail Manager über die SES-Konsole beginnen.

Erste Schritte mit Mail Manager mithilfe der Amazon SES SES-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich Mail Manager und anschließend auf der Mail Manager-Übersichtsseite eine der Schaltflächen Erste Schritte mit Mail Manager aus.
3. Wählen Sie auf der Seite Get up auf der Karte Eine Verkehrsrichtlinie erstellen die Option Verkehrsrichtlinie erstellen aus.

    a. Schließen Sie den Workflow auf der Seite Verkehrsrichtlinie erstellen ab. Weitere Informationen finden Sie unterthe section called “Erstellung von Verkehrsrichtlinien und Richtlinienerklärungen (Konsole)”.

    b. Nachdem Sie Ihre ersten Verkehrsrichtlinien und Richtlinienerklärungen erstellt haben, verwenden Sie die Zurück-Schaltfläche Ihres Browsers, um zur Seite Get Setup zurückzukehren, oder wählen Sie im linken Navigationsbereich unter Mail Manager die Option Get Setup aus.
4. Wählen Sie auf der Seite Get Setup auf der Karte Regelsatz erstellen die Option Regelsatz erstellen aus.

    a. Schließen Sie den Workflow auf der Seite Regelsatz erstellen ab. Weitere Informationen finden Sie unterthe section called “Regelsätze und Regeln erstellen (Konsole)”.

    b. Nachdem Sie Ihren ersten Regelsatz und Regeln erstellt haben, verwenden Sie die Zurück-Schaltfläche Ihres Browsers, um zur Seite Get Setup zurückzukehren, oder wählen Sie Get Setup unter Mail Manager im linken Navigationsbereich aus.

5. Nachdem Sie Ihre erste Verkehrsrichtlinie und Ihren ersten Regelsatz erstellt haben, können Sie Ihren ersten Eingangsendpunkt erstellen. Wählen Sie auf der Seite Get set up auf der Karte Create an Ingress Endpoint (Eingangsendpunkt erstellen) die Option Ingress-Endpoint erstellen aus.

    - Teil des Workflows auf der Seite E-Mail-Eingangsendpunkt besteht darin, dem Eingangsendpunkt die soeben erstellte Datenverkehrsrichtlinie und den Regelsatz zuzuweisen. Weitere Informationen finden Sie unter. the section called “Einen Ingress-Endpunkt (Konsole) erstellen”

Nachdem Sie Ihren ersten Eingangsendpunkt erstellt haben, können Sie Mail Manager verwenden und dessen weitere Funktionen wie SMTP-Relays und E-Mail-Archivierung nutzen. Sie können auch zusätzliche Eingangsendpunkte mit eigenen Datenverkehrsrichtlinien und Regelsätzen einrichten, um die Verwaltung all Ihrer eingehenden E-Mails weiter anzupassen.

Eingangsendpunkte

Ein Eingangsendpunkt ist die wichtigste Infrastrukturkomponente in Mail Manager, die Ihre E-Mails empfängt, weiterleitet und verwaltet. Dabei werden von Ihnen konfigurierte Richtlinien und Regeln verwendet, um festzulegen, welche E-Mails abgelehnt, welche zugelassen werden sollen und auf welche reagiert werden soll.

Jeder Eingangsendpunkt hat seine eigene Datenverkehrsrichtlinie, mit der festgelegt wird, welche E-Mails blockiert oder zugelassen werden sollen, und einen eigenen Regelsatz, um Aktionen für die E-Mail auszuführen, die Sie zulassen. Wenn Sie also mehrere Eingangsendpunkte erstellen, können Sie jeden einzelnen delegieren, um bestimmte Arten von E-Mails zu verwalten und weiterzuleiten. Diese Granularität hilft Ihnen beim Aufbau eines E-Mail-Managementsystems, das auf Ihre Geschäftsanforderungen zugeschnitten ist.

Erforderlicher Workflow zur Erstellung eines Eingangsendpunkts

Zum Zeitpunkt der Erstellung Ihres Eingangsendpunkts müssen Sie ihm eine Verkehrsrichtlinie und einen Regelsatz zuweisen, die bereits erstellt wurden. Daher sollte der Arbeitsablauf für die Erstellung eines Eingangsendpunkts in der folgenden Reihenfolge ablaufen:

1. Erstellen Sie zunächst eine Verkehrsrichtlinie, um festzulegen, welche E-Mail Sie blockieren oder zulassen möchten. Details hierzu finden Sie unter the section called “Erstellung von Verkehrsrichtlinien und Richtlinienerklärungen (Konsole)”.

2. Erstellen Sie als Nächstes einen Regelsatz für die Ausführung von Aktionen an der E-Mail, die Sie zulassen. Details hierzu finden Sie unter the section called “Regelsätze und Regeln erstellen (Konsole)”.
3. Erstellen Sie abschließend Ihren Eingangsendpunkt und weisen Sie ihm die Verkehrsrichtlinie und den Regelsatz zu, den Sie gerade erstellt haben, oder alle anderen, die Sie zuvor erstellt haben.

Sobald Sie Ihren Eingangsendpunkt erstellt haben, müssen Sie ihn mit der Umgebung konfigurieren, die Sie für den E-Mail-Empfang verwenden, unabhängig davon, ob es sich dabei um die Konfiguration eines lokalen SMTP-Clients oder eines webbasierten DNS-Domain-Hosts handelt. Dies wird weiter unten unter erörtert. the section called “Konfiguration öffentlicher Endgeräte”

Konfiguration Ihrer Umgebung für die Verwendung eines Ingress-Endpunkts

SES unterstützt sowohl öffentliche Endpunkte als auch Amazon Virtual Private Cloud (VPC) -Endpunkte, damit Eingangsendpunkte eingehende E-Mails annehmen können. In den folgenden Abschnitten wird erklärt, wie Sie Ihren Eingangsendpunkt so konfigurieren, dass er eine dieser Optionen verwendet.

Themen

- Empfangen von E-Mails über die öffentlichen Endpunkte
- Empfangen von E-Mails über Amazon VPC-Endpunkte

Empfangen von E-Mails über die öffentlichen Endpunkte

Verwenden des „A“ -Datensatzes

Wenn Sie einen Eingangsendpunkt erstellen, wird ein A-Eintrag für den Endpunkt generiert und sein Wert wird auf dem Übersichtsbildschirm des Eingangsendpunkts in der SES-Konsole angezeigt. Die Art und Weise, wie Sie den Wert dieses Datensatzes verwenden, hängt von der Art des von Ihnen erstellten Endpunkts und Ihrem Anwendungsfall ab:

- Offener Endpunkt — An Ihre Domain gesendete E-Mails werden direkt an Ihren Eingangsendpunkt weitergeleitet — eine Authentifizierung ist nicht erforderlich.
  - Kopieren Sie den Wert des „A“ -Eintrags und fügen Sie ihn entweder direkt in die SMTP-Konfiguration eines SMTP-Clients vor Ort oder in einen MX-Eintrag für Ihre Domain in Ihrer DNS-Konfiguration ein.
  - Unterstützter Port: 25

  - Unterstützt STARTTLS: Ja
- Authentifizierter Endpunkt — E-Mails, die an Ihre Domain gesendet werden, müssen von autorisierten Absendern stammen, mit denen Sie Ihre SMTP-Anmeldeinformationen geteilt haben, z. B. von Ihren lokalen E-Mail-Servern.
  - Kopieren Sie den Wert des „A“ -Eintrags und fügen Sie ihn zusammen mit Ihrem Benutzernamen und Passwort direkt in die SMTP-Konfiguration eines SMTP-Clients vor Ort ein.
  - Unterstützte Ports: 25, 587 (RFC 2476)
  - Unterstützt STARTTLS: Ja
- mTLS-Endpunkt — An Ihre Domain gesendete E-Mails müssen von Clients stammen, die ein TLS-Client-Zertifikat vorlegen, das von einer der Zertifizierungsstellen (CAs) im Trust Store des Eingangsendpunkts signiert wurde. Siehe the section called “mTLS-Authentifizierung”.
  - Kopieren Sie den Wert des „A“ -Eintrags und fügen Sie ihn direkt in die SMTP-Konfiguration eines SMTP-Clients vor Ort ein.
  - Unterstützter Port: 25
  - Unterstützt STARTTLS: Ja

Wenn Sie in Ihrer Konfiguration einen MX-Eintrag verwenden, denken Sie daran, dass zwar jeder DNS-Anbieter über unterschiedliche Verfahren und Schnittstellen für die Konfiguration von Einträgen verfügt, die wichtigsten Informationen, die Sie in Ihre DNS-Einstellungen eingeben müssen, jedoch im folgenden Beispiel aufgeführt sind:

Alle an recipient@marketing.example.com gesendeten E-Mails werden an Ihren Eingangsendpunkt gesendet, da Sie den A-Eintrag des Eingangsendpunkts als Wert für einen MX-Eintrag in den DNS-Einstellungen Ihrer Domain eingegeben haben:

- Domäne — `marketing.example.com`
- MX-Eintragswert — `890123abcdef.ghijk.mail-manager-smtp.amazonaws.com` (Dies ist der „A“ -Datensatzwert, der von Ihrem Eingangsendpunkt kopiert wurde.)
- Priorität — `10`

Verbindung zum authentifizierten Endpunkt herstellen

Für die autorisierten Absender, mit denen Sie Ihre SMTP-Anmeldeinformationen geteilt haben, um eine Verbindung zu Ihrem authentifizierten Endpunkt herzustellen, müssen die folgenden Protokolle

für den Benutzernamen und das Passwort befolgt werden, um eine erfolgreiche Verbindung zum Server herzustellen:

- Benutzername — Dies ist die ID des Eingangsendpunkts und muss in Base64 codiert sein. (Siehe Schritt 11. in den Konsolenprozeduren erfahren Sie, wie Sie die Eingangs-Endpunkt-ID finden.)
- Passwort — Dieses Passwort wird bei der Erstellung des Eingangsendpunkts verwendet und muss in Base64 codiert sein.

Das folgende Beispiel zeigt einen typischen Austausch zwischen SMTP-AUTH-Server und -Client, der eine Verbindung herstellt:

```
S: 250 AUTH LOGIN PLAIN
C: AUTH LOGIN
S: 334 VXNlcm5hbWU6
C: SW5ncmVzc1BvaW50
S: 334 UGFzc3dvcmQ6
C: SW5ncmVzc1Bhc3N3b3Jk
S: 235 Authentication successful
```

Dieses Beispiel enthält die folgenden Eigenschaften:

- `S`bedeutet „Server“ — der SMTP-Server, der Nachrichten akzeptiert.
- `C`bedeutet „Client“ — der SMTP-Client, der eine Verbindung zum Server herstellt und Nachrichten an den Server sendet.
- `250 AUTH LOGIN PLAIN`ist eine Antwort des Servers mit unterstützten AUTH-MethodenAUTH PLAIN, AUTH LOGIN oder der Absender könnte eine der beiden Methoden wählen und SMTP-Befehle senden, die der SMTP Service Extension for Authentication-Spezifikation RFC 2554 entsprechen. `AUTH LOGIN`wird hier verwendet.
- `334 VXNlcm5hbWU6`— Server fragt nach dem Benutzernamen in Base64.
- `SW5ncmVzc1BvaW50`— Der Client antwortet mit der Ingress-Endpunkt-ID in Base64.
- `334 UGFzc3dvcmQ6`— Server fordert zur Eingabe des Passworts in Base64 auf.
- `SW5ncmVzc1Bhc3N3b3Jk`— Der Client antwortet mit einem Passwort für den Eingangsendpunkt in Base64.

Empfangen von E-Mails über Amazon VPC-Endpunkte

Zusätzlich zu öffentlichen Eingangsendpunkten können Sie VPC-Endpunkte mit SES-Eingangsendpunkten für die sichere, private E-Mail-Aufnahme innerhalb Ihrer privaten Netzwerkinfrastruktur verwenden.

Unterschiede in der Konfiguration im Vergleich zur Verwendung von Endpunkten für öffentliche Eingänge

- Der A-Eintrag, der normalerweise für öffentliche Endpunkte verfügbar ist, wird nicht bereitgestellt.
- Sie müssen mithilfe der von Ihrem VPC-Endpunkt bereitgestellten DNS-Namen eine Verbindung zum Eingangsendpunkt herstellen.
- Alle Verbindungen verwenden private Netzwerke innerhalb Ihrer VPC.

Arten von Eingangsendpunkten, die über VPC-Endpunkte unterstützt werden

SES unterstützt zwei Arten von Eingangspunkten über VPC-Endpunkte:

- Eingangsendpunkt öffnen — E-Mails, die an Ihre Domain gesendet werden, werden direkt über den VPC-Endpunkt weitergeleitet, ohne dass eine Absenderauthentifizierung erforderlich ist.

  Anforderungen an die Konfiguration:

  - Erstellen Sie einen privaten Open-Ingress-Endpunkt, indem Sie ihn einer VPC-Endpunkt-ID zuordnen, die Sie besitzen.
  - Unterstützte Ports: 25, 587
  - Unterstützt STARTTLS: Ja
- Authentifizierter Eingangsendpunkt — E-Mails, die an Ihre Domain gesendet werden, müssen von autorisierten Absendern stammen, mit denen Sie Ihre SMTP-Anmeldeinformationen geteilt haben, z. B. von Ihren lokalen E-Mail-Servern.

  Anforderungen an die Konfiguration:

  - Erstellen Sie einen privaten authentifizierten Eingangsendpunkt, indem Sie ihn einer VPC-Endpunkt-ID zuordnen, die Sie besitzen.
  - Unterstützte Ports: 25, 587
  - Unterstützt STARTTLS: Ja

  - Die Authentifizierung verwendet denselben Base64-codierten Benutzernamen und Passwortmechanismus wie bei öffentlich authentifizierten Endpunkten.
- mTLS-Eingangsendpunkt — An Ihre Domain gesendete E-Mails müssen von Clients stammen, die ein TLS-Client-Zertifikat vorlegen, das von einem der Clients CAs im Trust Store des Eingangsendpunkts signiert wurde. Siehe the section called “mTLS-Authentifizierung”.

  Anforderungen an die Konfiguration:

  - Erstellen Sie einen privaten mTLS-Eingangsendpunkt, indem Sie ihn einer VPC-Endpunkt-ID zuordnen, die Sie besitzen.
  - Unterstützte Ports: 25, 587
  - Unterstützt STARTTLS: Ja

VPC-Endpunktanforderungen

Um einen VPC-Endpunkt mit einem SES-Ingress-Endpunkt zu verwenden, müssen die folgenden Anforderungen erfüllt sein:

- Der VPC-Endpunkt muss aktiv und verfügbar sein.
- Der VPC-Endpunkt muss demselben AWS Konto gehören wie der Eingangsendpunkt (kontoübergreifender Zugriff wird nicht unterstützt).
- Der VPC-Endpunkt muss für den entsprechenden Dienstnamen basierend auf dem Typ des Eingangsendpunkts erstellt werden:
  - Eingangsendpunkt öffnen — `com.amazonaws.region.mail-manager-smtp.open`
  - Authentifizierter Eingangsendpunkt — `com.amazonaws.region.mail-manager-smtp.auth`
  - mTLS-Eingangsendpunkt — `com.amazonaws.region.mail-manager-smtp.mtls`
  - FIPS-Endpunkt für offenen Eingangszugriff — `com.amazonaws.region.mail-manager-smtp.open.fips`
  - FIPS-authentifizierter Eingangsendpunkt — `com.amazonaws.region.mail-manager-smtp.auth.fips`
  - FIPS-MTLS-Eingangsendpunkt — `com.amazonaws.region.mail-manager-smtp.mtls.fips`

Wichtige Hinweise zur Konfiguration

- One-to-one Beziehung — Jeder VPC-Endpunkt kann nur einem einzelnen Eingangsendpunkt zugeordnet werden. Sie können denselben VPC-Endpunkt nicht für mehrere Eingangsendpunkte verwenden.
- Keine VPC-Endpunktrichtlinien — Im Gegensatz zu anderen AWS Diensten unterstützen VPC-Endpunkte, die mit Eingangsendpunkten verwendet werden, keine VPC-Endpunktrichtlinien. SES überprüft automatisch, ob der Besitzer des VPC-Endpunkts und der Eigentümer des Eingangsendpunkts dasselbe Konto sind. AWS
- Nur privates DNS — Alle vom VPC-Endpunkt bereitgestellten DNS-Namen sind private DNS-Namen, auf die nur innerhalb Ihrer VPC zugegriffen werden kann.
- Validierung zum Zeitpunkt der Erstellung — SES führt während der Ressourcenerstellung eine Validierung durch, um sicherzustellen, dass der VPC-Endpunkt alle Anforderungen erfüllt.
- Die TLS-Richtlinie muss mit VPC VPC-Endpunktdienst übereinstimmen — Beim Erstellen eines privaten Eingangsendpunkts muss der TLS-Richtlinienwert dem VPC-Endpunktdiensttyp entsprechen. Ein Eingangsendpunkt mit einer `FIPS` TLS-Richtlinie muss einen FIPS-VPC-Endpunktdienst verwenden, und ein Eingangsendpunkt mit einer `REQUIRED` oder `OPTIONAL` TLS-Richtlinie muss einen Nicht-FIPS-VPC-Endpunktdienst verwenden. Sie können nicht gemischt werden.

Über einen VPC-Endpunkt eine Verbindung zu Ihrem Ingress-Endpunkt herstellen

Nachdem Sie Ihren VPC-Endpunkt und Ihren Ingress-Endpunkt konfiguriert haben:

1. Rufen Sie die für Ihren VPC-Endpunkt generierten DNS-Namen ab.
2. Konfigurieren Sie Ihre SMTP-Clients oder E-Mail-Server so, dass sie diese DNS-Namen für die Verbindung verwenden.
3. Wenn Sie einen authentifizierten Endpunkt verwenden, konfigurieren Sie Ihre SMTP-Clients mit den entsprechenden Base64-codierten Anmeldeinformationen, die für Ihren authentifizierten Eingangsendpunkt verwendet werden.

TLS-Richtlinie für Eingangsendpunkte

Die TLS-Richtlinie für einen Eingangsendpunkt steuert, ob SMTP-Clients, die eine Verbindung herstellen, beim Senden von E-Mails an Ihren Endpunkt die TLS-Verschlüsselung verwenden müssen. Sie können beim Erstellen eines Eingangsendpunkts mithilfe der `CreateIngressPoint` API eine TLS-Richtlinie angeben und diese später mithilfe der API ändern. `UpdateIngressPoint`

Die Standard-TLS-Richtlinie hängt von Ihrer Region ab: Sie `FIPS` ist die Standardrichtlinie in den USA und Kanada und `REQUIRED` die Standardrichtlinie in allen anderen Regionen.

Alle Ingress-Endpunktverbindungen verwenden opportunistisches TLS über den Befehl STARTTLS. Die Verbindung beginnt als Klartext und wird auf TLS aktualisiert, wenn der Client, der die Verbindung herstellt, dies unterstützt. Implizites TLS (TLS Wrapper), bei dem die Verbindung verschlüsselt beginnt, wird nicht unterstützt.

Die folgenden TLS-Richtlinienwerte sind verfügbar:

- FIPS — Erfordert TLS-Verschlüsselung mit FIPS-validierten kryptografischen Modulen. Dies ist die Standardeinstellung in den Regionen USA und Kanada und nur in diesen Regionen verfügbar.
- ERFORDERLICH — SMTP-Clients, die eine Verbindung herstellen, müssen TLS-Verschlüsselung verwenden. Verbindungen, die kein TLS verwenden, werden abgelehnt. Dies ist die Standardeinstellung in Regionen außerhalb der USA und Kanada.
- OPTIONAL — TLS-Verschlüsselung wird unterstützt, ist aber nicht erforderlich. SMTP-Clients, die eine Verbindung herstellen, können E-Mails mit oder ohne TLS senden.

Verfügbarkeit nach Eingangsendpunkttyp

Nicht alle TLS-Richtlinienwerte sind für jede Kombination aus Eingangsendpunkttyp und Netzwerkkonfiguration gültig:

- FIPS — Kann mit allen Eingangsendpunkttypen (offen, authentifiziert und mTLS) sowohl in öffentlichen als auch in privaten Netzwerken verwendet werden, jedoch nur in den Regionen USA und Kanada. Einmal festgelegt, `FIPS` kann er nicht durch ein Update auf einen anderen Wert geändert werden. Wenn Sie eine andere TLS-Richtlinie benötigen, müssen Sie einen neuen Eingangsendpunkt erstellen.
- ERFORDERLICH — Kann mit allen Eingangs-Endpunkttypen in allen Regionen verwendet werden. Für authentifizierte Endpunkte und mTLS-Eingangsendpunkte in öffentlichen Netzwerken kann dies jedoch nur bei der Erstellung festgelegt werden — es `REQUIRED` kann nicht durch ein Update geändert werden. Kann bei offenen Eingangsendpunkten (öffentlich oder privat) und authentifizierten oder mTLS-Eingangsendpunkten in privaten Netzwerken bei der Erstellung festgelegt und durch ein Update geändert werden. `REQUIRED` Beachten Sie, dass `REQUIRED` dies nicht für authentifizierte oder mTLS-Eingangsendpunkte in öffentlichen Netzwerken in den Regionen USA und Kanada verfügbar ist, wo `FIPS` stattdessen verwendet wird.

- OPTIONAL — Kann mit offenen Eingangsendpunkten in öffentlichen und privaten Netzwerken und mit authentifizierten Eingangsendpunkten in privaten Netzwerken verwendet werden. `OPTIONAL`ist nicht für mTLS-Eingangsendpunkte und nicht für authentifizierte Eingangsendpunkte in öffentlichen Netzwerken verfügbar.

Regeln für die Änderung der TLS-Richtlinie

Bei der Aktualisierung der TLS-Richtlinie auf einem vorhandenen Eingangsendpunkt gelten die folgenden Regeln:

- `FIPS`kann nach der Erstellung nicht geändert werden.
- Bei offenen Eingangsendpunkten und authentifizierten Eingangsendpunkten in privaten Netzwerken können Sie zwischen und wechseln. `REQUIRED` `OPTIONAL`
- Für mTLS-Eingangsendpunkte und authentifizierte Eingangsendpunkte in öffentlichen Netzwerken kann die TLS-Richtlinie nach der Erstellung nicht geändert werden.

Gegenseitige TLS-Authentifizierung (mTLS) für Eingangsendpunkte

Für die gegenseitige TLS-Authentifizierung (mTLS) müssen SMTP-Clients, die eine Verbindung herstellen, ein TLS-Client-Zertifikat vorlegen, das von einer der Zertifizierungsstellen (CAs) im Trust Store des Eingangsendpunkts signiert wurde. Nur Clients mit vertrauenswürdigen Zertifikaten können E-Mails an Ihren Endpunkt senden.

Um einen mTLS-Eingangsendpunkt zu erstellen, wählen Sie `MTLS` als Eingangsendpunkttyp und geben Sie `TrustStore` im `IngressPointConfiguration` API-Parameter ein `TlsAuthConfiguration` enthaltendes a an. `CreateIngressPoint`

Konfiguration des Vertrauensspeichers

Der Trust Store definiert, welche Client-Zertifikate von Ihrem Eingangsendpunkt akzeptiert werden. Dies umfasst die folgenden Felder:

- CAContent(erforderlich) — Ein Zertifikatspaket der Zertifizierungsstelle (CA) im PEM-Format. Dieses Paket enthält die CA-Zertifikate, die zur Validierung von Client-Zertifikaten verwendet werden. Sie können mehrere CA-Zertifikate bis zu 500 KB in einem einzigen Paket zusammenfassen.

- CrlContent(optional) — Eine Zertifikatssperrliste (CRL) im PEM-Format. Falls angegeben, werden Client-Zertifikate, die auf der CRL erscheinen, zurückgewiesen, auch wenn sie von einer vertrauenswürdigen Zertifizierungsstelle signiert wurden. Bis zu 500 KB.
- KmsKeyArn(optional) — Der ARN eines vom AWS KMS Kunden verwalteten Schlüssels (CMK), der zur Verschlüsselung der Trust Store-Daten verwendet wird. Wenn nicht angegeben, wird ein AWS verwalteter Schlüssel verwendet. Bei Verwendung eines CMK muss die Schlüsselrichtlinie SES die Verwendung des Schlüssels ermöglichen. Siehe KMS-Schlüsselrichtlinie für vom Kunden verwaltete Schlüssel (CMK) für den MTLs Trust Store.

Abgelaufene Zertifikate gelten als ungültig und werden in Verbindungen nicht akzeptiert. SES filtert außerdem abgelaufene CA-Zertifikate und Sperrlisten für abgelaufene Zertifikate (CRLs) aus Ihrem Trust Store heraus. Wenn eine CRL abläuft, wird das mit dieser CRL verknüpfte CA-Zertifikat ebenfalls aus dem Trust Store entfernt, was bedeutet, dass von dieser CA signierte Clients keine Verbindung mehr herstellen können, bis Sie eine aktualisierte CRL angeben.

Verwendung von Client-Zertifikatsattributen in Regelbedingungen

Wenn ein Client mit einem gültigen Zertifikat eine Verbindung zu einem mTLS-Eingangsendpunkt herstellt, werden die Zertifikatsattribute (wie die Felder Common Name, Seriennummer und Alternativer Betreffname) für die Verwendung in Regelbedingungen als Zeichenfolgenausdrücke zur Verfügung gestellt. Auf diese Weise können Sie E-Mails basierend auf der Identität des verbindenden Clients weiterleiten, filtern oder bearbeiten. Die vollständige Liste der verfügbaren Attribute finden Sie in der Referenz zu den Regelbedingungen.

Einen Ingress-Endpunkt in der SES-Konsole erstellen

Das folgende Verfahren zeigt Ihnen, wie Sie die Ingress-Endpunktseite in der SES-Konsole verwenden, um Eingangsendpunkte zu erstellen und die bereits erstellten zu verwalten.

So erstellen und verwalten Sie Ingress-Endpoints mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Mail Manager die Option Ingress Endpoints aus.
3. Wählen Sie auf der Seite Ingress-Endpoints die Option Ingress-Endpoint erstellen aus.
4. Geben Sie auf der Seite Neuen Eingangsendpunkt erstellen einen eindeutigen Namen für Ihren Eingangsendpunkt ein.

5. Wählen Sie aus, ob es sich um einen offenen, authentifizierten oder mTLS-Endpunkt handeln soll.

   - Wenn Sie Authentifiziert wählen, wählen Sie entweder SMTP-Passwort und geben Sie ein Passwort ein (das mit autorisierten Absendern geteilt werden soll) oder Geheim und wählen Sie eines Ihrer Geheimnisse aus Secret ARN aus. Wenn Sie ein zuvor erstelltes Geheimnis auswählen, muss es die in den folgenden Schritten angegebenen Richtlinien für die Erstellung eines neuen Geheimnisses enthalten.
   - Wenn Sie mTLS wählen, müssen Sie eine Trust-Store-Konfiguration angeben, die Ihr CA-Zertifikatspaket enthält. Optional können Sie auch eine Zertifikatssperrliste und einen AWS KMS Schlüssel angeben. Siehe the section called “mTLS-Authentifizierung”.
   - Sie haben die Möglichkeit, ein neues Geheimnis zu erstellen, indem Sie Create new wählen. Daraufhin wird die AWS Secrets Manager Konsole geöffnet, in der Sie mit der Erstellung eines neuen Schlüssels fortfahren können:

   a. Wählen Sie unter Geheimtyp die Option Anderer Geheimtyp aus.

   b. Geben Sie im Feld Schlüssel/Wert-Paar `password` den Schlüssel und Ihr aktuelles Passwort als Wert ein.

      > **Note**
      >
      > Für Schlüssel müssen Sie nur Folgendes eingeben `password` (alles andere führt dazu, dass die Authentifizierung fehlschlägt).

   c. Wählen Sie unter Verschlüsselungsschlüssel die Option Neuen Schlüssel hinzufügen aus, um einen vom Kunden verwalteten KMS-Schlüssel (CMK) zu erstellen. Die AWS KMS Konsole wird geöffnet.

   d. Wählen Sie auf der Seite „Vom Kunden verwaltete Schlüssel“ die Option Schlüssel erstellen aus.

   e. Behalten Sie die Standardwerte auf der Seite Schlüssel konfigurieren bei und wählen Sie Weiter.

   f. Geben Sie im Feld Alias einen Namen für Ihren Schlüssel ein (optional können Sie eine Beschreibung und ein Tag hinzufügen), gefolgt von Weiter.

   g. Wählen Sie unter Schlüsseladministratoren, gefolgt von Weiter, alle Benutzer (außer Ihnen selbst) oder Rollen aus, denen Sie die Verwaltung des Schlüssels gestatten möchten.

h. Wählen Sie unter Hauptbenutzer gefolgt von Weiter alle Benutzer (außer Ihnen selbst) oder Rollen aus, denen Sie die Verwendung des Schlüssels gestatten möchten.

i. Kopieren Sie den JSON-Texteditor und fügen Sie ihn auf der `"statement"` Ebene KMS-CMK-Richtlinie in den JSON-Texteditor für Schlüsselrichtlinien ein, indem Sie ihn als zusätzliche Anweisung hinzufügen, die durch ein Komma getrennt ist. Ersetzen Sie die Region und die Kontonummer durch Ihre eigene.

j. Wählen Sie Finish (Abschließen).

k. Wählen Sie den Tab Ihres Browsers aus, auf dem die Seite Neues Geheimnis AWS Secrets Manager speichern geöffnet ist, und klicken Sie auf das Aktualisierungssymbol (kreisförmiger Pfeil) neben dem Feld Verschlüsselungsschlüssel. Klicken Sie dann in das Feld und wählen Sie Ihren neu erstellten Schlüssel aus.

l. Geben Sie auf der Seite Geheimen Schlüssel konfigurieren einen Namen in das Feld Geheimer Name ein.

m. Wählen Sie unter Ressourcenberechtigungen die Option Berechtigungen bearbeiten aus.

n. Kopieren Sie den JSON-Texteditor und fügen Sie ihn Secrets-Ressourcenrichtlinie in den JSON-Texteditor für Ressourcenberechtigungen ein. Ersetzen Sie die Region und die Kontonummer durch Ihre eigenen. (Achten Sie darauf, jeglichen Beispielcode im Editor zu löschen.)

o. Wählen Sie Speichern gefolgt von Weiter.

p. Konfigurieren Sie optional die Rotation gefolgt von Weiter.

q. Überprüfe und speichere dein neues Geheimnis, indem du Speichern auswählst.

r. Wählen Sie die Registerkarte Ihres Browsers aus, auf der die SES-Seite Create new ingress endpoint geöffnet ist, wählen Sie Liste aktualisieren und wählen Sie dann Ihr neu erstelltes Geheimnis in Secret ARN aus.

6. Wählen Sie einen Regelsatz aus, der die Regelaktionen enthält, die Sie für die E-Mail ausführen möchten, die Sie zulassen.

7. Wählen Sie eine Verkehrsrichtlinie aus, um festzulegen, welche E-Mail Sie blockieren oder zulassen möchten.

8. Wählen Sie aus, ob es sich um ein öffentliches oder ein privates Netzwerk handeln soll.

   - Wählen Sie für ein öffentliches Netzwerk entweder IPv4die reine Adressierung oder die Dualstack - (IPv4 und IPv6) Adressierung.
   - Wählen Sie für ein privates Netzwerk einen VPC-Endpunkt aus, den Sie mit autorisierten Absendern in demselben Konto geteilt haben, z. B. mit IAM-Benutzern oder -Rollen, oder

geben Sie ihn ein. Optional können Sie einen neuen VPC-Endpunkt erstellen, indem Sie VPC-Endpunkt erstellen wählen, um die Amazon VPC-Konsole zu öffnen.

9. Wählen Sie eine TLS-Richtlinie für Ihren Eingangsendpunkt aus. Die Standardeinstellung hängt von Ihrer Region ab. TLS-Richtlinie Einzelheiten zu verfügbaren Werten und Einschränkungen finden Sie unter.
10. Wählen Sie Ingress-Endpunkt erstellen aus.
11. In den allgemeinen Details wird „Bereitstellung“ angezeigt, während Ihr Eingangsendpunkt erstellt wird. Aktualisieren Sie die Seite, bis „Aktiv“ angezeigt wird und das Feld einen Wert enthält. ARecord Kopieren Sie den Datensatzwert „A“ und fügen Sie ihn in Ihre DNS-Konfiguration oder Ihren SMTP-Client ein, wie unter beschrieben. Konfiguration öffentlicher Endgeräte
12. Direkt über dem Container „Allgemeine Details“ auf der Konsole befindet sich eine große, unbeschriftete Zahl mit dem Präfix „inp“ (ebenfalls im Breadcrumb-Trail oben auf der Seite repliziert), z. B. inp-1abc2de3fghi4jkl5mnop6qr. Dies wird als Eingangsendpunkt-ID bezeichnet. Ihr Wert wird als Benutzername für die Anmeldung bei Ihrem Ingress-Server verwendet. (Sie müssen dies Ihren autorisierten Absendern mitteilen, um eine Verbindung zu Ihrem Endpunkt herzustellen.)
13. Sie können die Ingress-Endpoints, die Sie bereits erstellt haben, auf der Seite Ingress-Endpoints anzeigen und verwalten. Wenn es einen Eingangsendpunkt gibt, den Sie entfernen möchten, wählen Sie das entsprechende Optionsfeld und anschließend Löschen aus.
14. Um einen Eingangsendpunkt zu bearbeiten, wählen Sie seinen Namen aus, um die zugehörige Übersichtsseite zu öffnen:

    - Sie können den aktiven Status oder die TLS-Richtlinie des Endpunkts (für unterstützte Konfigurationen) ändern, indem Sie unter Allgemeine Details Bearbeiten und anschließend Änderungen speichern auswählen.
    - Sie können einen anderen Regelsatz oder eine andere Verkehrsrichtlinie auswählen, indem Sie entweder im Regelsatz oder in der Verkehrsrichtlinie Bearbeiten und anschließend Änderungen speichern auswählen.

Verkehrspolitik und Grundsatzerklärungen

Eine Verkehrsrichtlinie ist ein Container für Richtlinienerklärungen, die Sie einem Eingangsendpunkt zuweisen, sodass dieser die eingehenden E-Mails sortieren kann, indem er bestimmte Arten von E-

Mails zulässt oder blockiert, sofern die Bedingungen der Richtlinienanweisungen erfüllt sind. Eine Verkehrsrichtlinie kann von mehreren Eingangsendpunkten verwendet werden.

> **Tip**
>
> Sie können sich eine Verkehrsrichtlinie als „Filtersatz“ und eine Richtlinienerklärung als „Filter“ vorstellen. Die Verkehrsrichtlinie (Filtersatz) enthält Richtlinien (Filter), mit denen Sie Ihre eingehenden E-Mails filtern.

Wenn Sie eine Verkehrsrichtlinie erstellen, haben Sie die Möglichkeit, eine maximale Nachrichtengröße (in Byte) festzulegen. Wenn eine Nachricht diese Größe überschreitet, wird sie verworfen. Sie können die Standardaktion der Richtlinie auch so festlegen, dass E-Mails zugelassen oder blockiert werden, die nicht den Bedingungen Ihrer Richtlinienerklärungen entsprechen. Stellen Sie sich das als „Alles abfangen“ -Aktion für die Verkehrsrichtlinie vor.

Richtlinienerklärungen werden außerdem entweder mit einer Zulassen- oder Blockierungsaktion erstellt, die ergriffen wird, wenn die Bedingungen der Anweisungen erfüllt sind. Sie erstellen die Bedingungen, indem Sie eine E-Mail-Eigenschaft und einen Bedingungsoperator für einen von Ihnen eingegebenen Wert auswählen, der mit der eingehenden Nachricht übereinstimmen muss, bevor die Richtlinienanweisung sie zulässt oder blockiert. Jede Richtlinienerklärung kann mehrere Bedingungen haben.

Eine Verkehrsrichtlinie kann mehrere Richtlinienerklärungen enthalten und sie in einer Reihenfolge ausführen, die auf der impliziten Hierarchie der E-Mail-Bewertung basiert:

- Blockierende Richtlinienanweisungen — Diese Anweisungen werden zuerst ausgewertet und blockieren alle Nachrichten, die die Bedingungen der Anweisung erfüllen.
- Zulässige Grundsatzerklärungen — Diese Aussagen werden als Nächstes bewertet und lassen jede Nachricht zu, die die Bedingungen der Erklärung erfüllt.
- Standardaktion der Verkehrsrichtlinie — Der Rest der Nachrichten, die nicht den Richtlinienbestimmungen entsprechen, werden je nachdem, wie Sie diesen Parameter definiert haben, zugelassen oder blockiert.
- Maximale Nachrichtengröße — Wenn dieser optionale Parameter festgelegt ist, werden alle Nachrichten, die diese Größe überschreiten, verworfen.

Eine Verkehrsrichtlinie ist eine unabhängige Ressource, die von mehr als einem Eingangsendpunkt verwendet werden kann. Richtlinienerklärungen gehören jedoch ausschließlich zu der Verkehrsrichtlinie, in der sie erstellt wurden. Daher müssen Sie zuerst eine Verkehrsrichtlinie erstellen oder eine bestehende bearbeiten, bevor Sie Richtlinienerklärungen erstellen können, um die E-Mails zu bewerten, die an Ihren Eingangsendpunkt gelangen.

Das Verfahren im nächsten Abschnitt erklärt, wie Sie Verkehrsrichtlinien und deren Richtlinienerklärungen in der SES-Konsole erstellen.

Erstellen von Verkehrsrichtlinien und Richtlinienerklärungen in der SES-Konsole

Das folgende Verfahren zeigt Ihnen, wie Sie die Seite mit den Verkehrsrichtlinien in der SES-Konsole verwenden, um Verkehrsrichtlinien und deren Richtlinienerklärungen zu erstellen und die bereits erstellten zu verwalten.

So erstellen und verwalten Sie Verkehrsrichtlinien und Richtlinienerklärungen mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Mail Manager die Option Verkehrsrichtlinien aus.
3. Wählen Sie auf der Seite Verkehrsrichtlinien die Option Verkehrsrichtlinie erstellen aus.
4. Geben Sie auf der Seite Verkehrsrichtlinie erstellen einen eindeutigen Namen für Ihre Verkehrsrichtlinie ein.
5. (Optional) Wenn Sie Nachrichten, die eine bestimmte Größe überschreiten, verwerfen möchten, geben Sie einen Wert in Byte in das Feld Maximale Nachrichtengröße ein.
6. Wählen Sie unter Standardaktion aus, ob die Datenverkehrsrichtlinie Nachrichten zulassen oder ablehnen (blockieren) soll, die nicht den Bedingungen Ihrer Richtlinienerklärungen entsprechen (nicht adressiert werden).
7. Wählen Sie Neue Richtlinienerklärung hinzufügen aus, um eine Erklärung für Ihre Verkehrsrichtlinie zu erstellen.
8. Wählen Sie entweder Zulassen oder Verweigern (Sperren) für die Aktion, die ausgeführt werden soll, wenn die Bedingungen der Erklärung erfüllt sind.
9. Erstellen Sie eine Bedingung, indem Sie eine E-Mail-Eigenschaft und einen Bedingungsoperator für den eingegebenen Wert auswählen. Wählen Sie Neue Bedingung hinzufügen aus, wenn Sie dieser Richtlinienerklärung weitere Bedingungen hinzufügen möchten. Weitere Informationen

zu einer Bedingungseigenschaft und ihren Operatoren und gültigen Werten finden Sie in der Referenz zu den Bedingungen der Richtlinienerklärung.

- Wenn Sie ein E-Mail-Add-On abonniert haben, können Sie es hier als E-Mail-Eigenschaft auswählen.
- Datenverkehrsrichtlinien, die mit Eingangsendpunkten IPv6 oder Dual-Stack-Eingangsendpunkten verknüpft sind, bewerten keine E-Mail-Add-On-Bedingungen und wenden diese auch nicht auf Nachrichten an, die über Verbindungen empfangen werden. IPv6 Die Bedingungen für das Hinzufügen von E-Mails gelten nur für Nachrichten, die über IPv4 Verbindungen auf Dual-Stack-Endpunkten empfangen werden.

10. Wenn Sie weitere Richtlinienerklärungen und Bedingungen hinzufügen möchten, wiederholen Sie die obigen Schritte 7 bis 9.
11. Wenn Sie mit der Erstellung von Richtlinienerklärungen und deren Bedingungen fertig sind, wählen Sie Verkehrsrichtlinie erstellen aus.
12. Sie können die Verkehrsrichtlinien, die Sie bereits erstellt haben, auf der Seite Verkehrsrichtlinien einsehen und verwalten. Wenn Sie eine Verkehrsrichtlinie entfernen möchten, wählen Sie das entsprechende Optionsfeld und anschließend Löschen aus.
13. Um die Eigenschaften einer Verkehrsrichtlinie oder eine ihrer Richtlinienerklärungen zu bearbeiten, wählen Sie ihren Namen aus, um die zugehörige Übersichtsseite zu öffnen. Wählen Sie von hier aus Bearbeiten aus.
14. In den Details zur Verkehrsrichtlinie können Sie die maximale Nachrichtengröße und die Standardaktion ändern.
15. In jedem Container mit Richtlinien-Anweisungen können Sie die allow/deny Eigenschaft ändern und alle Bedingungen bearbeiten. Sie können auch Richtlinienerklärungen und Bedingungen entfernen sowie neue hinzufügen.
16. Wenn Sie mit all Ihren Änderungen fertig sind, speichern Sie Ihre Änderungen, indem Sie Änderungen speichern auswählen.

Referenz für die Bedingungen der Grundsatzerklärung

Bedingungen der Grundsatzerklärung

In der folgenden Referenztabelle sind alle Eigenschaften von Richtlinienanweisungen aufgeführt, die für die Erstellung einer Grundsatzerklärung zur Verfügung stehen. Wenn Sie den Ausdruckstyp einer Eigenschaft auswählen, gelangen Sie zu der entsprechenden Referenzseite in der SES Mail

Manager API-Referenz, auf der alle verfügbaren Operatoren und gültigen Werte für diese Eigenschaft aufgeführt sind.

Bedingungen der Grundsatzerklärung: Eigenschaften, Operatoren und Werte

Eigenschaft	Ausdruckstyp
Empfängeradresse Abusix Mail Intelligence (falls abonniert) • Gelistet am Spamhaus-Domain-Sperrliste (falls abonniert) • Gelistet auf	Gültige Operatoren und Werte für Zeichenkettenausdrücke
IP-Bereich des Absenders	Gültige Operatoren und Werte für IP-Ausdrücke
Version des TLS-Protokolls	Gültige Operatoren und Werte für TLS-Protokollausdrücke
Abusix Mail Intelligence (falls abonniert) • Ist gelistet Spamhaus-Domain-Sperrliste (falls abonniert) • Ist aufgeführt	Gültige Operatoren und Werte für boolesche Ausdrücke

Adressabgleich und Unteradressierung von Empfängeradressen

Die Eigenschaft Empfängeradresse verwendet die vollständige Empfängeradresse des SMTP-Umschlags genau so, wie sie empfangen wurde, einschließlich aller Unteradressenerweiterungen (auch bekannt als „Plus-Adressierung“). Wenn beispielsweise eine Nachricht gesendet wird`user+tag@example.com`, lautet die in der Richtlinienerklärung angegebene Empfängeradresse „Nein“. `user+tag@example.com` `user@example.com` Das bedeutet, dass das Targeting einer `EQUALS` `CONTAINS` `user@example.com` Oder-Regel nicht zutrifft`user+tag@example.com`. Wenn Sie alle unteradressierten Varianten

einer Adresse abgleichen müssen, sollten Sie die Verwendung einer Adressliste mit Platzhaltereinträgen (z. B.) in Betracht ziehen. `user*@example.com` Alternativ kann `ENDS_WITH` mit der Domäne (z. B.`@example.com`) ein umfassenderer Abgleich auf Domänenebene erfolgen.

Regelsätze und Regeln

Regelsätze sind Container für Regeln, die Sie einem Eingangsendpunkt zuweisen, sodass dieser Aktionen für E-Mails ausführen kann, die gemäß der Datenverkehrsrichtlinie des Eingangsendpunkts zugelassen sind. Ein Regelsatz kann von mehreren Eingangsendpunkten verwendet werden.

Regeln teilen Ihrem Eingangsendpunkt mit, wie er mit eingehenden E-Mails umgehen soll, indem sie die in der Regel definierten Aktionen ausführen, wenn Nachrichten die Bedingungen der Regel erfüllen. Jede Regel kann mehrere Bedingungen und Aktionen haben. Die Regeln, die Sie innerhalb eines Regelsatzes erstellen, werden in der Reihenfolge ausgeführt, die Sie innerhalb des Regelsatzes angeben.

Sie erstellen die Bedingungen der Regel, indem Sie eine E-Mail-Eigenschaft und einen Bedingungsoperator für einen von Ihnen eingegebenen Wert auswählen, der mit der Nachricht übereinstimmen muss, bevor die Regel ihre Aktionen ausführt. Sie definieren die auszuführenden Aktionen sowie deren Ausführungsreihenfolge.

Für eine größere Granularität können Ihre Regeln auch Ausnahmen enthalten, die ähnlich wie Bedingungen definiert sind. In diesem Fall definieren Sie jedoch eine Bedingung, der die Nachricht nicht entsprechen darf. Bedingungen und Ausnahmen funktionieren unabhängig voneinander. Sie können eine Regel mit nur Ausnahmen erstellen, wenn Sie möchten, aber auch Bedingungen und Ausnahmen mischen.

Da Regeln innerhalb eines Regelsatzes sehr detailliert definiert werden können, soll die folgende Liste die Beziehung der Regelsatzkomponenten veranschaulichen:

- Regelsätze enthalten:
  - Regeln — Sie können die Reihenfolge definieren, in der die Regeln innerhalb des Regelsatzes ausgeführt werden.

    Regeln enthalten:
    - Bedingungen — Die Regel gilt, wenn die Nachricht der Bewertung der Bedingung (en) entspricht; und wenn die Regel Ausnahmen enthält, siehe unten.

- Ausnahmen — Die Regel gilt, wenn die Nachricht nicht der Bewertung der Ausnahme (n) entspricht und wenn die Regel Bedingungen enthält, siehe oben.
- Aktionen — Aktionen werden ausgelöst, wenn die Regel gilt — alle Bedingungen sind erfüllt und keine der Ausnahmen.

  Sie können die Reihenfolge definieren, in der die Aktionen innerhalb der Regel ausgeführt werden.

Da jede Regel mehrere Bedingungen, Ausnahmen und Aktionen haben kann und Sie die Reihenfolge festlegen können, in der Regeln und Aktionen ausgeführt werden, können Sie auf diese Weise eine maßgeschneiderte und automatisierte E-Mail-Verwaltungslösung erstellen, die auf Ihre spezifischen Geschäftsanforderungen zugeschnitten ist.

Ein Regelsatz ist eine unabhängige Ressource, die von mehr als einem Eingangsendpunkt verwendet werden kann. Regeln gehören jedoch ausschließlich zu dem Regelsatz, in dem sie erstellt wurden. Daher müssen Sie zuerst einen Regelsatz erstellen oder einen vorhandenen bearbeiten, bevor Sie Regeln erstellen können, die auf die E-Mail reagieren, die an Ihren Eingangsendpunkt gelangt.

Das Verfahren im nächsten Abschnitt führt Sie durch die Erstellung von Regelsätzen und deren Regeln in der SES-Konsole.

Regelsätze und Regeln in der SES-Konsole erstellen

Das folgende Verfahren zeigt Ihnen, wie Sie die Seite Regelsätze in der SES-Konsole verwenden, um Regelsätze und deren Regeln zu erstellen und die bereits erstellten zu verwalten.

So erstellen und verwalten Sie Regelsätze und Regeln mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Mail Manager die Option Regelsätze aus.
3. Wählen Sie auf der Seite Regelsätze die Option Regelsatz erstellen aus und geben Sie einen eindeutigen Namen für Ihren Regelsatz ein.
4. Wählen Sie auf der Übersichtsseite des Regelsatzes Bearbeiten und dann auf der Bearbeitungsseite Neue Regel erstellen aus.
5. Geben Sie in der Seitenleiste mit den Regeldetails einen eindeutigen Namen für Ihre Regel ein.

6. Wählen Sie Neue Bedingung hinzufügen aus, um eine Bedingung zu erstellen, der die Nachricht entsprechen muss, oder aktivieren Sie das Kästchen AUSSER bei: gefolgt von Neue Ausnahme hinzufügen, um eine Bedingung zu erstellen, der die Nachricht nicht entsprechen darf.
7. Erstellen Sie die Bedingung oder Ausnahme, indem Sie eine E-Mail-Eigenschaft und einen Bedingungsoperator für den eingegebenen Wert auswählen. Wählen Sie Neue Bedingung hinzufügen oder Neue Ausnahme hinzufügen, wenn Sie dieser Regel weitere Bedingungen oder Ausnahmen hinzufügen möchten. Weitere Informationen zu einer Bedingungseigenschaft und ihren Operatoren und gültigen Werten finden Sie in der Referenz zu Regelbedingungen.

   - Wenn Sie ein E-Mail-Add-On abonniert haben, können Sie es hier als E-Mail-Eigenschaft auswählen.
8. Wählen Sie Neue Aktion hinzufügen aus, um die Aktion zu definieren, die ausgeführt werden soll, wenn die Bedingungen der Regel erfüllt sind. and/or Ausnahmen sind nicht erfüllt. Um weitere auszuführende Aktionen hinzuzufügen, wählen Sie Neue Aktion hinzufügen aus. Wenn Sie zwei oder mehr Aktionen erstellen, werden up/down Pfeile angezeigt, sodass Sie die Reihenfolge der Ausführung festlegen können.

   > **Note**
   >
   > Um eine dieser Regelaktionen ausführen zu können, müssen Sie die entsprechende Berechtigungsrichtlinie für Ihr Konto aktiviert haben. Andernfalls schlägt die Regelaktion fehl.
9. Wenden Sie die Berechtigungsrichtlinie für jede dieser Aktionen direkt im Bereich Regeldetails an, nachdem Sie die Aktion ausgewählt haben:

   a. Wählen Sie im Feld IAM-Rolle die Option Neue Rolle erstellen aus und geben Sie einen Namen gefolgt von Rolle erstellen ein. (Die IAM-Vertrauensrichtlinie für diese Rolle wird automatisch im Hintergrund generiert.)

   b. Da die IAM-Vertrauensrichtlinie automatisch generiert wurde, müssen Sie der Rolle nur die Berechtigungsrichtlinie der Aktion hinzufügen. Wählen Sie im Feld IAM-Rolle die Option Rolle anzeigen aus, um die IAM-Konsole zu öffnen.

   c. Wählen Sie auf der Registerkarte „Berechtigungen“ die Option „Berechtigungen hinzufügen“ und dann „Inline-Richtlinie erstellen“ aus.

   d. Wählen Sie auf der Seite „Berechtigungen angeben“ im Richtlinien-Editor die Option JSON aus.

e. Kopieren Sie die entsprechende Richtlinie, fügen Sie Berechtigungsrichtlinien für Mail Manager sie aus dem Richtlinien-Editor ein und ersetzen Sie die Daten im roten Text durch Ihre eigenen. (Achten Sie darauf, jeglichen Beispielcode im Editor zu löschen.)

f. Wählen Sie Weiter aus.

g. Überprüfen und erstellen Sie Ihre Berechtigungsrichtlinie für die IAM-Rolle, indem Sie Richtlinie erstellen wählen.

h. Wählen Sie die Registerkarte Ihres Browsers aus, auf der die Seite Regelsatz bearbeiten von SES Mail Manager geöffnet ist, und fahren Sie mit den verbleibenden Schritten zur Erstellung von Regeln fort.

10. Wenn Sie mit der Erstellung der Bedingungen, Ausnahmen und Aktionen für die Regel fertig sind, speichern Sie sie in ihrem Regelsatz, indem Sie im Bereich Regelsatz bearbeiten auf der linken Seite die Option Regelsatz speichern wählen.
11. Wenn Sie dem Regelsatz weitere Regeln hinzufügen möchten, wiederholen Sie die obigen Schritte 4 bis 9.

    - Wenn Sie zwei oder mehr Regeln erstellen, werden in der Spalte „Neu anordnen“ des Regelsatzes up/down Pfeile angezeigt, sodass Sie die Ausführungsreihenfolge festlegen können.

12. Sie können die Regelsätze, die Sie bereits erstellt haben, auf der Seite Regelsätze anzeigen und verwalten. Wenn Sie einen Regelsatz entfernen möchten, wählen Sie das entsprechende Optionsfeld und anschließend Löschen aus.
13. Um einen Regelsatz zu bearbeiten, wählen Sie seinen Namen aus, um seine Übersichtsseite zu öffnen. Wählen Sie dann Bearbeiten, um die Ausführung der Regeln neu zu ordnen, weitere Regeln hinzuzufügen, indem Sie Neue Regel erstellen wählen, oder eine Regel löschen, indem Sie das entsprechende Optionsfeld und dann Löschen auswählen.
14. Um eine Regel zu bearbeiten, wählen Sie das entsprechende Optionsfeld aus. In jedem Container in der Seitenleiste mit den Regeldetails können Sie alle Bedingungen oder Ausnahmen bearbeiten und die Aktionen ändern oder neu anordnen. Sie können auch Bedingungen, Ausnahmen und Aktionen entfernen sowie neue hinzufügen.
15. Wenn Sie mit all Ihren Änderungen fertig sind, speichern Sie Ihre Änderungen, indem Sie im Bereich Regelsatz bearbeiten auf der linken Seite die Option Regelsatz speichern auswählen.

Referenz für Regelbedingungen und Aktionen

Regelbedingungen

In der folgenden Referenztabelle sind alle Regeleigenschaften aufgeführt, die zum Erstellen einer Regelbedingung (oder Ausnahme) verfügbar sind und nach ihrem Ausdruckstyp kategorisiert sind. Regeleigenschaften, die denselben Ausdruckstyp verwenden, haben auch dieselben Operatoren und Werte. Wenn Sie den Ausdruckstyp einer Eigenschaft auswählen, gelangen Sie zu der entsprechenden Referenzseite in der SES Mail Manager API-Referenz, auf der alle verfügbaren Operatoren und gültigen Werte für diese Eigenschaft aufgeführt sind.

Regelbedingungen: Eigenschaften, Operatoren und Werte

Eigenschaft	Ausdruckstyp
Von der Adresse	
Zur Adresse	
CC-Adresse	
E-Mail von	
Empfängeradresse	
Betreff	
Hallo	
MIME-Header	Gültige Operatoren und Werte für Zeichenfolgenausdrücke
Client-Zertifikatattribut (nur mTLS-Eingangsendpunkte) • Seriennummer • Gemeinsamer Name • Land • Ort • Organisation • Organisatorische Einheit • Status • Alternativer Name des Betreffs	

Eigenschaft	Ausdruckstyp
Vade Advanced Email Security (falls abonniert) • Kategorie • Urteil Trend Micro Virus Scanning (falls abonniert) • Kategorie	
IP-Bereich	Gültige Operatoren und Werte für IP-Ausdrücke
Maximale Größe der Nachricht	Gültige Operatoren und Werte für Zahlenausdrücke
DKIM SPF	Gültige Operatoren und Werte für Urteilsausdrücke
TLS Mit TLS verpackt Quittung lesen Vade Advanced Email Security (falls abonniert) • Ist bestanden Trend Micro Virus Scanning (falls abonniert) • Ist bestanden	Gültige Operatoren und Werte für boolesche Ausdrücke
DMARC-Richtlinie	Gültige Operatoren und Werte für DMARC-Ausdrücke

> **Adressabgleich und Subadressierung von Empfängeradressen**
>
> Die Eigenschaft Empfängeradresse verwendet die vollständige Empfängeradresse des SMTP-Umschlags genau so, wie sie empfangen wurde, einschließlich aller Unteradressenerweiterungen (auch bekannt als „Plus-Adressierung“). Wenn beispielsweise eine Nachricht an gesendet wird, lautet die `user+tag@example.com` in der Regelbedingung ausgewertete Empfängeradresse „Nein“. `user+tag@example.com` `user@example.com` Das bedeutet, dass das Targeting einer `EQUALS` `CONTAINS` `user@example.com` Oder-Regel nicht zutrifft`user+tag@example.com`. Wenn Sie alle unteradressierten Varianten einer Adresse abgleichen müssen, sollten Sie die Verwendung einer Adressliste mit Platzhaltereinträgen (z. B.) in Betracht ziehen. `user*@example.com` Alternativ kann `ENDS_WITH` mit der Domäne (z. B.`@example.com`) ein umfassenderer Abgleich auf Domänenebene erfolgen.

Aktionen regeln

In der folgenden Referenztabelle sind alle Regelaktionen aufgeführt, die ergriffen werden können, wenn die Bedingungen einer Regel erfüllt sind oder ihre Ausnahmen nicht erfüllt sind. Wenn Sie eine Aktion auswählen, werden Sie zur Referenzseite der Aktion in der SES Mail Manager API-Referenz weitergeleitet, auf der die Parameter und ihre Formate für die Aktion aufgeführt sind. In der Tabelle werden die Aktionsnamen verwendet, die in der Mail Manager-Konsole übernommen wurden. Die API-Namen können geringfügig abweichen.

> **Note**
>
> In einigen API-Referenzen wird es einen *`ActionFailurePolicy`* Parameter geben, der entweder auf Continue oder Drop gesetzt werden kann, falls die Aktion fehlschlägt. Dies gilt nur, wenn die API verwendet wird; bei Verwendung der Konsole *`ActionFailurePolicy`* wurde er auf den Standardwert Continue gesetzt.

Regelaktionen: Aktionen und Parameter

Aktionen und ihre Parameter	Description
Schreiben Sie auf S3	Schreibt den MIME-Inhalt der E-Mail in einen S3-Bucket.

Aktionen und ihre Parameter	Description
SMTP-Relay	Leitet die E-Mail über SMTP an einen anderen bestimmten SMTP-Server weiter.
Archiv	Archiviert die E-Mail, indem sie an ein Amazon SES SES-Archiv gesendet wird.
Header hinzufügen	Fügt der empfangenen E-Mail einen benutzerd efinierten Header hinzu.
E-Mail-Empfänger schreiben um	Ersetzt die Empfänger des E-Mail-Umschlags durch die angegebene Empfängerliste. Wenn die Bedingung dieser Aktion nur für eine Untergruppe von Empfängern gilt, werden nur diese Empfänger ersetzt.
An das Postfach WorkMail liefern	Liefert die E-Mail an ein WorkMail Amazon-Po stfach.
An Q Business liefern	Sendet eine E-Mail an eine Amazon Q Business-Anwendung zur Aufnahme in deren Wissensdatenbank.
Auf SNS veröffentlichen	Veröffentlicht den E-Mail-Inhalt zu einem Amazon SNS SNS-Thema.
Ins Internet senden	Verwendet SES, um die E-Mail an die Empfänger auf der Empfängerliste der E-Mail zu senden.
Bounce	Leitet die E-Mail zurück, indem eine Bounce-An twort an den Absender zurückgesendet wird.

Aktionen und ihre Parameter	Description
Lambda-Funktion aufrufen	Ruft eine AWS Lambda Funktion zur Verarbeitung der E-Mail auf. Das Lambda-Payload-Format entspricht dem E-Mail-Empfang von Amazon SES, wie unter Benachrichtigungsinhalte beschrieben. Weitere Informationen finden Sie unter Beispielanwendungsfälle. Codebeispiele finden Sie unter Beispiele für Lambda-Funktionen.
Löschen	Wenn diese Aktion bei E-Mails mit mehreren Empfängern auf einen oder mehrere (aber nicht alle) dieser Empfänger zutrifft, werden diese aus der Empfängerliste der E-Mail gelöscht, und die weitere Verarbeitung der Regeln gilt für die verbleibenden Empfänger. Wenn diese Aktion für alle Empfänger gilt, wird die Regelverarbeitung beendet, da alle Empfänger aus der Empfängerliste gestrichen werden und die E-Mail nicht erhalten.

SMTP-Relay

Da Mail Manager zwischen Ihrer E-Mail-Umgebung (wie Microsoft 365, Google Workspace oder On-Premise Exchange) und dem Internet eingesetzt wird, verwendet Mail Manager SMTP-Relays, um eingehende E-Mails, die von Mail Manager verarbeitet werden, an Ihre E-Mail-Umgebung weiterzuleiten. Es kann auch ausgehende E-Mails an eine andere E-Mail-Infrastruktur weiterleiten, z. B. an einen anderen Exchange-Server oder ein E-Mail-Gateway eines Drittanbieters, bevor sie an die Endempfänger gesendet werden.

Ein SMTP-Relay ist eine wichtige Komponente Ihrer E-Mail-Infrastruktur. Es ist für die effiziente Weiterleitung von E-Mails zwischen Servern verantwortlich, sofern dies durch eine in einem Regelsatz definierte Regelaktion vorgesehen ist.

Insbesondere kann ein SMTP-Relay eingehende E-Mails zwischen SES Mail Manager und einer externen E-Mail-Infrastruktur wie Exchange, lokalen E-Mail-Gateways oder E-Mail-Gateways

von Drittanbietern und anderen weiterleiten. Eingehende E-Mails an einen Eingangsendpunkt werden nach einer Regel verarbeitet, die die angegebenen E-Mails an das angegebene SMTP-Relay weiterleitet, das sie wiederum an die im SMTP-Relay definierte externe E-Mail-Infrastruktur weiterleitet.

Wenn Ihr Eingangsendpunkt E-Mails empfängt, bestimmt er anhand einer Verkehrsrichtlinie, welche E-Mails blockiert oder zugelassen werden sollen. Die E-Mail, die Sie zulassen, wird einem Regelsatz übergeben, der bedingte Regeln anwendet, um die Aktionen auszuführen, die Sie für bestimmte E-Mail-Typen definiert haben. Eine der Regelaktionen, die Sie definieren können, ist SMTPRelay Aktion. Wenn Sie diese Aktion auswählen, wird die E-Mail an den externen SMTP-Server weitergeleitet, der in Ihrem SMTP-Relay definiert ist.

Sie könnten die SMTPRelay Aktion beispielsweise verwenden, um E-Mails von Ihrem Eingangsendpunkt an Ihren lokalen Microsoft Exchange Server zu senden. Sie würden Ihren Exchange-Server so einrichten, dass er über einen öffentlichen SMTP-Endpunkt verfügt, auf den nur mit bestimmten Anmeldeinformationen zugegriffen werden kann. Wenn Sie das SMTP-Relay erstellen, geben Sie den Servernamen, den Port und die Anmeldeinformationen Ihres Exchange-Servers ein und geben Ihrem SMTP-Relay einen eindeutigen Namen, z. B. "“. RelayToMyExchangeServer Anschließend erstellen Sie im Regelsatz Ihres Eingangsendpunkts eine Regel, die besagt: „Wenn die Absenderadresse 'gmail.com' enthält, führen Sie die SMTPRelay Aktion mit dem SMTP-Relay namens durch“. RelayToMyExchangeServer

> **Note**
>
> Alle SMTP-Endpunkte, die Sie mit Amazon SES SMTP Relay konfigurieren, müssen öffentlich sein, da private SMTP-Endpunkte nicht unterstützt werden.

Wenn nun eine E-Mail von gmail.com an Ihrem Eingangsendpunkt ankommt, löst die Regel die SMTPRelay Aktion aus und kontaktiert Ihren Exchange-Server mit den Anmeldeinformationen, die Sie bei der Erstellung Ihres SMTP-Relays angegeben haben, und übermittelt die E-Mail an Ihren Exchange-Server. Somit werden von gmail.com empfangene E-Mails an Ihren Exchange-Server weitergeleitet.

Sie müssen zuerst ein SMTP-Relay erstellen, bevor es in einer Regelaktion festgelegt werden kann. Das Verfahren im nächsten Abschnitt führt Sie durch die Erstellung eines SMTP-Relays in der SES-Konsole.

Erstellen eines SMTP-Relays in der SES-Konsole

Das folgende Verfahren zeigt Ihnen, wie Sie die Seite SMTP-Relays in der SES-Konsole verwenden, um SMTP-Relays zu erstellen und die bereits erstellten zu verwalten.

So erstellen und verwalten Sie SMTP-Relays mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Mail Manager die Option SMTP-Relays aus.
3. Wählen Sie auf der Seite SMTP-Relays die Option SMTP-Relay erstellen aus.
4. Geben Sie auf der Seite SMTP-Relay erstellen einen eindeutigen Namen für Ihr SMTP-Relay ein.
5. Je nachdem, ob Sie ein eingehendes (nicht authentifiziertes) oder ausgehendes (authentifiziertes) SMTP-Relay konfigurieren möchten, folgen Sie den jeweiligen Anweisungen:

   Inbound

   So konfigurieren Sie ein eingehendes SMTP-Relay

   1. Wenn SMTP-Relay als Eingangsgateway verwendet wird, um eingehende E-Mails, die von Mail Manager verarbeitet wurden, an Ihre externe E-Mail-Umgebung weiterzuleiten, müssen Sie zunächst die E-Mail-Hosting-Umgebung konfigurieren. Jeder E-Mail-Hosting-Anbieter hat zwar seine eigene grafische Oberfläche und seinen eigenen Konfigurationsablauf, aber die Prinzipien der Konfiguration für die Verwendung mit eingehenden Gateways, wie z. B. Ihrem Mail Manager-SMTP-Relay, sind ähnlich.

      Um dies zu verdeutlichen, haben wir in den folgenden Abschnitten Beispiele für die Konfiguration von Google Workspaces und Microsoft Office 365 für die Verwendung mit Ihrem SMTP-Relay als eingehendem Gateway bereitgestellt:

      - Google Workspaces einrichten
      - Microsoft Office 365 einrichten

      > **Note**
      >
      > Stellen Sie sicher, dass Ihre beabsichtigten Empfängerziele SES-verifizierte E-Mail-Identitäten sind. Wenn Sie beispielsweise E-Mails an die Empfänger

abc@example.com, admin@example.com, postmaster@acme.com und support@acme.com zustellen möchten, empfehlen wir Ihnen, die `acme.com` Domänen `example.com` und in SES zu verifizieren. Wenn ein Empfängerziel nicht verifiziert ist, versucht SES nicht, die E-Mail an den öffentlichen SMTP-Server zuzustellen.

2. Nachdem Sie Google Workspaces oder Microsoft Office 365 für die Verwendung mit eingehenden Gateways konfiguriert haben, geben Sie den Hostnamen des öffentlichen SMTP-Servers mit den folgenden Werten für Ihren Anbieter ein:

   - Google Workspaces: `aspmx.l.google.com`
   - Microsoft Office 365: `<your_domain>.mail.protection.outlook.com`

     Ersetzen Sie die Punkte in Ihrem Domainnamen durch „-“. Wenn Ihre Domain beispielsweise acme.com lautet, würden Sie Folgendes eingeben `acme-com.mail.protection.outlook.com`
3. Geben Sie die Portnummer 25 für den öffentlichen SMTP-Server ein.
4. Lassen Sie den Abschnitt Authentifizierung leer (wählen oder erstellen Sie keinen geheimen ARN).

Outbound

Um ein ausgehendes SMTP-Relay zu konfigurieren

1. Geben Sie den Hostnamen des öffentlichen SMTP-Servers ein, zu dem Ihr Relay eine Verbindung herstellen soll.
2. Geben Sie die Portnummer für den öffentlichen SMTP-Server ein.
3. Richten Sie die Authentifizierung für Ihren öffentlichen SMTP-Server ein, indem Sie eines Ihrer Secrets aus Secret ARN auswählen. Wenn Sie ein zuvor erstelltes Geheimnis auswählen, muss es die in den folgenden Schritten angegebenen Richtlinien zum Erstellen eines neuen Geheimnisses enthalten.

   - Sie haben die Möglichkeit, ein neues Geheimnis zu erstellen, indem Sie Neues erstellen wählen. Daraufhin wird die AWS Secrets Manager Konsole geöffnet, in der Sie mit der Erstellung eines neuen Schlüssels fortfahren können:

a. Wählen Sie unter Geheimtyp die Option Anderer Geheimtyp aus.

b. Geben Sie die folgenden Schlüssel und Werte in Schlüssel/Wert-Paaren ein:

Key (Schlüssel)	value
`username`	mein_benutzername
`password`	mein_Passwort

> **Note**
>
> Für beide Schlüssel müssen Sie nur `username` und `password` wie abgebildet eingeben (alles andere führt dazu, dass die Authentifizierung fehlschlägt). Geben Sie für die Werte Ihren eigenen Benutzernamen und Ihr Passwort ein.

c. Wählen Sie unter Verschlüsselungsschlüssel die Option Neuen Schlüssel hinzufügen aus, um einen vom Kunden verwalteten KMS-Schlüssel (CMK) zu erstellen. Die AWS KMS Konsole wird geöffnet.

d. Wählen Sie auf der Seite „Vom Kunden verwaltete Schlüssel“ die Option Schlüssel erstellen aus.

e. Behalten Sie die Standardwerte auf der Seite Schlüssel konfigurieren bei und wählen Sie Weiter aus.

f. Geben Sie im Feld Alias einen Namen für Ihren Schlüssel ein (optional können Sie eine Beschreibung und ein Tag hinzufügen), gefolgt von Weiter.

g. Wählen Sie unter Schlüsseladministratoren, gefolgt von Weiter, alle Benutzer (außer Ihnen selbst) oder Rollen aus, denen Sie die Verwaltung des Schlüssels gestatten möchten.

h. Wählen Sie unter Hauptbenutzer gefolgt von Weiter alle Benutzer (außer Ihnen selbst) oder Rollen aus, denen Sie die Verwendung des Schlüssels gestatten möchten.

i. Kopieren Sie den JSON-Texteditor und fügen Sie ihn auf der `"statement"` Ebene KMS-CMK-Richtlinie in den JSON-Texteditor für Schlüsselrichtlinien ein, indem

Sie ihn als zusätzliche Anweisung hinzufügen, die durch ein Komma getrennt ist. Ersetzen Sie die Region und die Kontonummer durch Ihre eigene.

j. Wählen Sie Finish (Abschließen).

k. Wählen Sie den Tab Ihres Browsers aus, auf dem die Seite Neues Geheimnis AWS Secrets Manager speichern geöffnet ist, und klicken Sie auf das Aktualisierungssymbol (kreisförmiger Pfeil) neben dem Feld Verschlüsselungsschlüssel. Klicken Sie dann in das Feld und wählen Sie Ihren neu erstellten Schlüssel aus.

l. Geben Sie auf der Seite Geheimen Schlüssel konfigurieren einen Namen in das Feld Geheimer Name ein.

m. Wählen Sie unter Ressourcenberechtigungen die Option Berechtigungen bearbeiten aus.

n. Kopieren Sie den JSON-Texteditor und fügen Sie ihn Secrets-Ressourcenrichtlinie in den JSON-Texteditor für Ressourcenberechtigungen ein. Ersetzen Sie die Region und die Kontonummer durch Ihre eigenen. (Achten Sie darauf, jeglichen Beispielcode im Editor zu löschen.)

o. Wählen Sie Speichern gefolgt von Weiter.

p. Konfigurieren Sie optional die Rotation gefolgt von Weiter.

q. Überprüfe und speichere dein neues Geheimnis, indem du Speichern auswählst.

r. Wählen Sie die Registerkarte Ihres Browsers aus, auf der die SES-Seite SMTP-Relay erstellen geöffnet ist, wählen Sie Liste aktualisieren und wählen Sie dann Ihr neu erstelltes Geheimnis in Secret ARN aus.

6. Wählen Sie SMTP-Relay erstellen aus.

7. Sie können die SMTP-Relays, die Sie bereits erstellt haben, auf der Seite SMTP-Relays anzeigen und verwalten. Wenn Sie ein SMTP-Relay entfernen möchten, wählen Sie das entsprechende Optionsfeld und anschließend Löschen aus.

8. Um ein SMTP-Relay zu bearbeiten, wählen Sie seinen Namen aus. Auf der Detailseite können Sie den Namen des Relays, den Namen, den Port und die Anmeldeinformationen des externen SMTP-Servers ändern, indem Sie auf die entsprechende Schaltfläche Bearbeiten oder Aktualisieren und anschließend auf Änderungen speichern klicken.

Einrichtung von Google Workspaces für eingehendes (nicht authentifiziertes) SMTP-Relay

Die folgende exemplarische Vorgehensweise zeigt Ihnen, wie Sie Google Workspaces so einrichten, dass es mit einem eingehenden (nicht authentifizierten) Mail Manager-SMTP-Relay funktioniert.

Voraussetzungen

- Zugriff auf die Google-Administratorkonsole (Google-Administratorkonsole > Apps > Google Workspace > Gmail).
- Zugriff auf den Domain-Nameserver, der die MX-Einträge für die Domains hostet, die für die Einrichtung von Mail Manager verwendet werden.

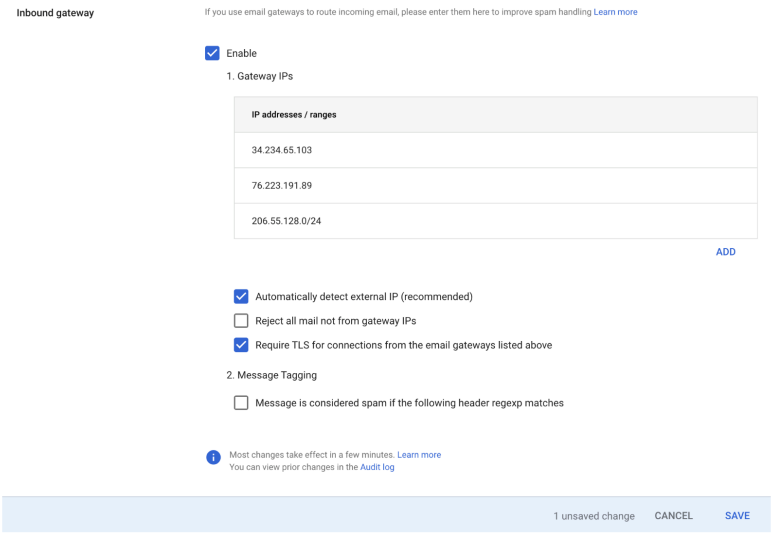
So richten Sie Google Workspaces für die Arbeit mit einem eingehenden SMTP-Relay ein

- Fügen Sie Mail Manager-IP-Adressen zur Konfiguration des Eingangs-Gateways hinzu

  a. Gehen Sie in der Google-Administratorkonsole zu Apps > Google Workspace > Gmail.

  b. Wählen Sie Spam, Phishing und Malware aus und wechseln Sie dann zur Konfiguration des Inbound-Gateways.

  c. Aktivieren Sie das Inbound-Gateway und konfigurieren Sie es mit den folgenden Details:



  - Wählen Sie unter Gateway IPs die Option Hinzufügen aus und fügen Sie den für Ihre Region IPs spezifischen Eingangsendpunkt aus der Tabelle der SMTP-Relay-IP-Bereiche hinzu.

- Wählen Sie Externe IP automatisch erkennen aus.
- Wählen Sie TLS erforderlich für Verbindungen von den oben aufgeführten E-Mail-Gateways aus.
- Wählen Sie unten im Dialogfeld Speichern aus, um die Konfiguration zu speichern. Nach dem Speichern zeigt die Administratorkonsole das Inbound-Gateway als aktiviert an.

Einrichten von Microsoft Office 365 für eingehendes (nicht authentifiziertes) SMTP-Relay

Die folgende exemplarische Vorgehensweise zeigt Ihnen, wie Sie Microsoft Office 365 so einrichten, dass es mit einem eingehenden (nicht authentifizierten) Mail Manager-SMTP-Relay funktioniert.

Voraussetzungen

- Zugriff auf das Microsoft Security Admin Center (Microsoft Security Admin Center > E-Mail und Zusammenarbeit > Richtlinien und Regeln > Bedrohungsrichtlinien).
- Zugriff auf den Domain-Nameserver, der die MX-Einträge für die Domains hostet, die für die Einrichtung von Mail Manager verwendet werden.

So richten Sie Microsoft Office 365 für die Arbeit mit einem eingehenden SMTP-Relay ein

1. Fügen Sie Mail Manager-IP-Adressen zur Zulassungsliste hinzu

   a. Gehen Sie im Microsoft Security Admin Center zu E-Mail und Zusammenarbeit > Richtlinien und Regeln > Bedrohungsrichtlinien.

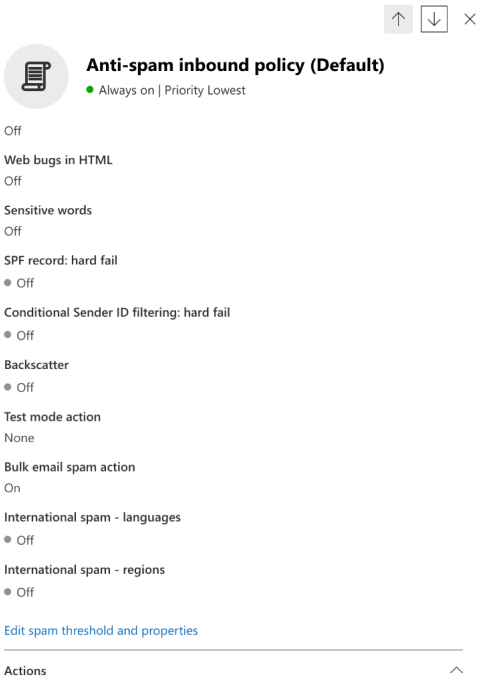
   b. Wählen Sie unter Richtlinien die Option Anti-Spam aus.

   c. Wählen Sie Verbindungsfilterrichtlinie gefolgt von Verbindungsfilterrichtlinie bearbeiten aus.

      - Fügen Sie im Dialogfeld Nachrichten aus den folgenden IP-Adressen oder dem folgenden Adressbereich immer zulassen den für Ihre Region IPs spezifischen Eingangsendpunkt aus der Tabelle SMTP-Relay-IP-Bereiche hinzu.
      - Wählen Sie Speichern aus.

   d. Kehren Sie zur Option Anti-Spam zurück und wählen Sie Anti-Spam-Richtlinie für eingehende E-Mails.

- Wählen Sie unten im Dialogfeld die Option Spam-Schwellenwert und Eigenschaften bearbeiten aus:



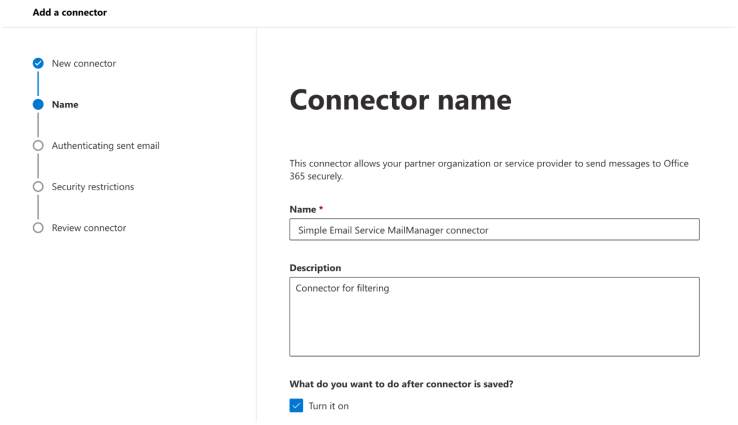
- Scrollen Sie zu Als Spam markieren und stellen Sie sicher, dass SPF record: hard fail auf Aus gesetzt ist.
- Wählen Sie Speichern aus.

2. Verbesserte Filterkonfiguration (empfohlen)

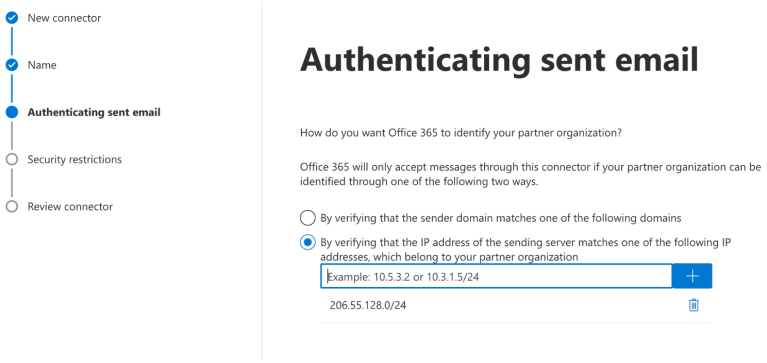
   Diese Option ermöglicht es Microsoft Office 365, die ursprüngliche Verbindungs-IP korrekt zu identifizieren, bevor die Nachricht von SES Mail Manager empfangen wurde.

   a. Erstellen Sie einen eingehenden Connector

   - Melden Sie sich im neuen Exchange Admin Center an und gehen Sie zu Mail Flow > Connectors.
   - Wählen Sie Konnektor hinzufügen aus.
   - Wählen Sie unter Verbindung von die Option Partnerorganisation und dann Weiter aus.
   - Füllen Sie die Felder wie folgt aus:
     - Name — Einfacher E-Mail-Dienst, Mail Manager-Connector
     - Beschreibung — Konnektor zum Filtern



- Klicken Sie auf Weiter.
- Wählen Sie unter Authentifizierung gesendeter E-Mails die Option Indem Sie überprüfen, ob die IP-Adresse des sendenden Servers mit einer der folgenden IP-Adressen übereinstimmt, die zu Ihrer Partnerorganisation gehören, aus und fügen Sie den für Ihre Region IPs spezifischen Eingangsendpunkt aus der Tabelle der SMTP-Relay-IP-Bereiche hinzu.

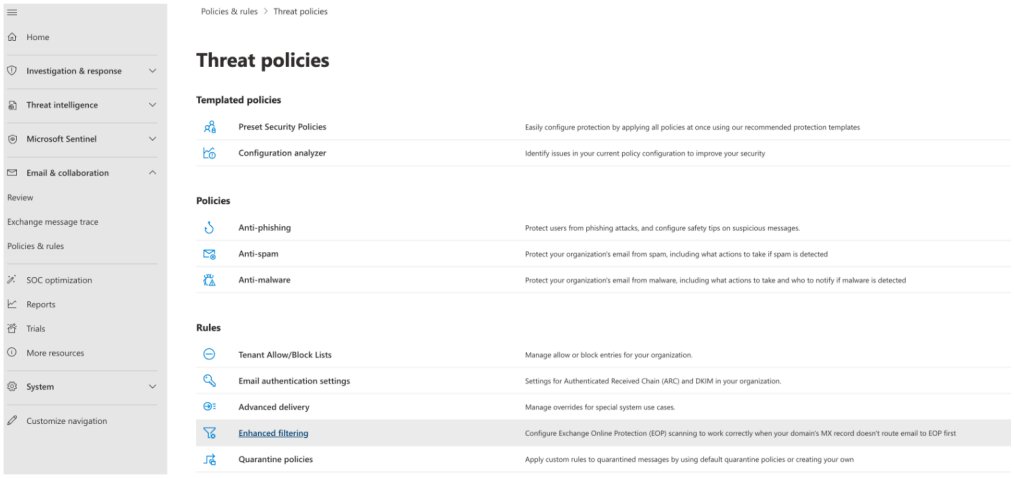


- Klicken Sie auf Weiter.
- Akzeptieren Sie unter Sicherheitseinschränkungen die Standardeinstellung E-Mail-Nachrichten ablehnen, wenn sie nicht über TLS gesendet werden, gefolgt von Weiter.
- Überprüfen Sie Ihre Einstellungen und wählen Sie Connector erstellen aus.

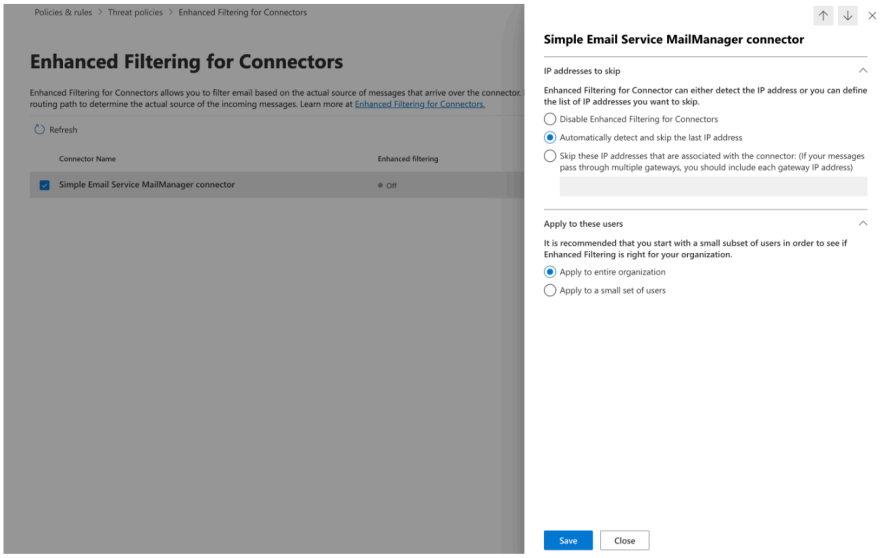
b. Aktivieren Sie die erweiterte Filterung

Nachdem der eingehende Connector konfiguriert wurde, müssen Sie die erweiterte Filterkonfiguration des Connectors im Microsoft Security Admin Center aktivieren.

- Gehen Sie im Microsoft Security Admin Center zu E-Mail und Zusammenarbeit > Richtlinien und Regeln > Bedrohungsrichtlinien.
- Wählen Sie unter Regeln die Option Erweiterte Filterung aus.



- Wählen Sie den Simple Email Service Mail Manager-Connector aus, den Sie zuvor erstellt haben, um seine Konfigurationsparameter zu bearbeiten.
- Wählen Sie sowohl Die letzte IP-Adresse automatisch erkennen und überspringen als auch Auf die gesamte Organisation anwenden aus.



- Wählen Sie Speichern.

Adresslisten

Adresslisten sind eine Mail Manager-Funktion, mit der Sie Listen mit E-Mail-Adressen und Domänen erstellen und verwalten können, die Sie in Verkehrsrichtlinien und Regelsätzen verwenden können, um eingehende E-Mails zu verarbeiten, je nachdem, ob der Empfänger oder Absender einer Nachricht zu einer bestimmten Liste gehört oder nicht. Adresslisten eignen sich für eine detailliertere

Steuerung des E-Mail-Verkehrs und tragen dazu bei, die Verwaltung komplexer E-Mail-Routing-Szenarien zu vereinfachen.

Was sind Adresslisten?

Adresslisten sind Container für E-Mail-Adressen und Domains, die Sie zum Filtern und Verarbeiten von E-Mail-Nachrichten verwenden können. Sie bieten eine bequeme Möglichkeit, zusammengehörige Adressen zu gruppieren und Routing-Regeln und Verkehrsrichtlinien gemeinsam anzuwenden.

Zu den wichtigsten Anwendungsfällen für Adresslisten gehören:

- Ablehnungslisten zum Blockieren bekannter Spam-Absender oder -Domänen
- Listen zulassen, um sicherzustellen, dass die Zustellung von vertrauenswürdigen Absendern erfolgt
- Empfängervalidierung zur frühzeitigen Ablehnung von E-Mails an nicht existierende Empfänger
- Rollenbasiertes Routing zur Anwendung verschiedener Regeln auf der Grundlage von Empfängerrollen
- Gruppenbasierte Richtlinien zur Durchsetzung von Richtlinien für bestimmte Benutzergruppen

Wie funktionieren Adresslisten

Adresslisten in SES optimieren die E-Mail-Verwaltung, indem sie es Ihnen ermöglichen, Sammlungen von E-Mail-Adressen und Domains zu erstellen und zu verwalten. Nach der Erstellung werden diese Listen durch Richtlinien und Regeln für den Datenverkehr in Ihre E-Mail-Workflows integriert.

Wenn SES eine E-Mail verarbeitet, überprüft es die entsprechende Adressliste, um festzustellen, ob der Absender oder Empfänger ein Mitglied ist. Auf der Grundlage dieser Mitgliedschaft und Ihrer konfigurierten Richtlinien und Regeln ergreift SES dann die entsprechenden Maßnahmen, z. B. das Weiterleiten, Filtern oder Ablehnen der E-Mail. Dieser Prozess ermöglicht eine effiziente und detaillierte Kontrolle über Ihren E-Mail-Verkehr.

Adresslisten einrichten

Themen

- Eine Adressliste erstellen und auffüllen
- Adresslisten verwalten

Eine Adressliste erstellen und auffüllen

Ein Teil der Erstellung einer Adressliste in der Konsole besteht darin, sie mit einer oder mehreren Adressen zu füllen. Mit dem Mail Manager APIs können Sie leere Adresslisten erstellen und diese später auffüllen. In diesem Abschnitt erfahren Sie anhand von Konsolenprozeduren und AWS CLI Beispielen, wie Sie beides tun können.

So erstellen Sie eine Adressliste und füllen sie aus:

1. Öffnen Sie die SES-Konsole unter. https://console.aws.amazon.com/ses/
2. Wählen Sie im Navigationsbereich unter Mail Manager die Option Adresslisten aus.
3. Wählen Sie Adressliste erstellen und geben Sie einen Namen in das Feld Adresslistenname ein.
4. Wählen Sie entweder Manuelle Eingabe oder Massen-Upload aus und folgen Sie den jeweiligen Schritten:
5. Für manuelle Eingabe — Geben Sie eine oder mehrere E-Mail-Adressen oder Domains in die Konsole ein.

   Wenn Sie das Sternchen (*) als Platzhalter verwenden, gelten die folgenden Formate:

   1. In der Adresse * ist nur einer zulässig:
      - Das * sollte entweder vor oder nach dem @ stehen, wenn es sich bei dem Eintrag um eine E-Mail-Adresse handelt.
      - Wenn * sich im lokalen Teil befindet, kann der lokale Teil null bis 19 Zeichen lang sein, mit Ausnahme von*.
      - Wenn * sich in der Domäne befindet, kann die Subdomänenebene zwischen 2 und 9 liegen, ohne die*.
   2. Beispiele für gültige Platzhalterformate:
      - *.domain1.com zu *.domain8.domain7... domain1.com
      - * @domain .com an 1234567890123456789* @domain .com
      - local@*.domain1.com zu local@*.domain8.domain7... domain1.com

   Platzhalter können verwendet werden, um E-Mail-Adressen unabhängig von Unteradressenerweiterungen (plus Adressierung) zuzuordnen. Beispielsweise entspricht das Hinzufügen `user*@example.com` zu einer Adressliste jeder Adresse, deren lokaler Teil

mit`user`, `user@example.com` `user+tag@example.com``username@example.com`, usw. beginnt.

6. Für den Massenupload — Wählen Sie Datei auswählen und wählen Sie eine CSV- oder JSON-Datei von Ihrem Computer aus, die die hochzuladenden Adressen enthält.

   Verwenden Sie für jeden Dateityp das im Beispiel gezeigte Format:

   1. Beispiel für eine CSV-Datei (Beachten Sie, dass der Header`address`,, erforderlich ist.):

      ```
      address
      user1@domain.com
      user2@*.domain.com
      *@domain.com
      ```

   2. Beispiel für eine JSON-Datei:

      ```
      {
        "items": [
          {
            "address": "user1@domain.com"
          },
          {
            "address": "user2@*.domain.com"
          },
          {
            "address": "*@domain.com"
          }
        ]
      }
      ```

7. Wenn Sie mit dem Hinzufügen von Adressen fertig sind oder eine Bulkdatei ausgewählt haben, wählen Sie Adressliste erstellen.

Verwenden von AWS CLI:

Erstellen Sie die Adressliste

```
aws mailmanager create-address-list --address-list-name "MyDenyList"
```

Füllen Sie die Adressliste aus:

- Einmaliger Upload

```
aws mailmanager register-member-to-address-list \
                --address-list-id al-123456789abc \
                --address "user@example.com"
```

- Massen-Upload

  Für Massen-Uploads müssen Sie zunächst einen Importjob erstellen, der entweder ein CSV- oder ein JSON-Format angibt:

```
aws mailmanager create-address-list-import-job \
                --address-list-id "al-123456789abc" \
                --name "MyImportJob" \
                --import-data-format ImportDataType=CSV
```

  Dadurch werden eine Job-ID und eine vorsignierte URL zurückgegeben. Verwenden Sie diese vorsignierte URL, um Ihre CSV- oder JSON-Datei in einen S3-Bucket hochzuladen, wie im folgenden Beispiel mit dem Befehl curl gezeigt:

```
curl -X PUT -T "/path/to/file" "pre-signed URL"
```

  Starten Sie nach dem Hochladen den Importjob mit der Job-ID, die im vorherigen Befehl zurückgegeben wurde:

```
aws mailmanager start-address-list-import-job --job-id "job-123456789"
```

Adresslisten verwalten

Sie können Adresslisten nach Bedarf aktualisieren, anzeigen und löschen.

Themen

- Eine Adressliste aktualisieren
- Details zur Adressliste anzeigen
- Löschen einer Adressliste

Eine Adressliste aktualisieren

Sie können eine Adressliste aktualisieren, indem Sie Adressen hinzufügen oder entfernen und optional Tags hinzufügen oder entfernen.

So aktualisieren Sie eine Adressliste:

1. Wählen Sie auf der Seite Adresslisten den Namen der Adressliste aus, die Sie bearbeiten möchten.
2. Um Adressen hinzuzufügen, wählen Sie E-Mail-Adresse hinzufügen und fahren Sie entweder mit der manuellen Eingabe oder dem Massenupload fort, wie unter beschriebenEine Adressliste erstellen und auffüllen.
3. Um Adressen zu entfernen, aktivieren Sie das Kontrollkästchen neben jeder Adresse, die Sie entfernen möchten, gefolgt von E-Mail-Adresse entfernen und bestätigen Sie den Löschvorgang.
4. (Optional) Fügen Sie Stichwörter zu Ihrer Adressliste hinzu oder entfernen Sie sie, indem Sie Stichwörter verwalten wählen.

Verwenden von AWS CLI:

Addition

```
aws mailmanager register-member-to-address-list \
                --address-list-id al-123456789abc \
                --address "user@example.com"
```

Remove

```
aws mailmanager deregister-member-from-address-list \
                --address-list-id al-123456789abc \
                --address "user@example.com"
```

Details zur Adressliste anzeigen

So zeigen Sie die Details der Adressliste an:

- Wählen Sie auf der Seite „Adresslisten“ den Namen einer Adressliste aus, um deren Details anzuzeigen.

Verwenden von AWS CLI:

```
aws mailmanager list-members-of-address-list --address-list-id al-123456789abc
```

Löschen einer Adressliste

Um eine Adressliste zu löschen:

1. Wählen Sie auf der Seite Adresslisten das Optionsfeld neben der Adressliste aus, die Sie löschen möchten, gefolgt von Löschen.
2. Bestätigen Sie das Löschen der Liste, indem Sie Bestätigen und dann Löschen eingeben.

Verwenden von AWS CLI:

```
aws mailmanager delete-address-list --address-list-id al-123456789abc
```

Verwenden von Adresslisten in Verkehrsrichtlinien und Regelsätzen

Adresslisten können in Aussagen zur Verkehrsrichtlinie und in Regelbedingungen verwendet werden, um E-Mails auf der Grundlage der Listenzugehörigkeit zu verarbeiten und so den E-Mail-Verkehr zu kontrollieren. Die folgenden Abschnitte enthalten ein Beispiel dafür, wie Adresslisten jeweils in einer Verkehrsrichtlinie und einem Regelsatz verwendet werden.

Themen

- Verwendung einer Adressliste in einer Erklärung zur Verkehrspolitik
- Verwenden einer Adressliste in einer Regel

Verwendung einer Adressliste in einer Erklärung zur Verkehrspolitik

Adresslisten können ausgewählt werden, wenn Sie die Bedingung einer Datenverkehrsrichtlinie so einrichten, dass E-Mails, die an Ihren Eingangsendpunkt gelangen, entweder zugelassen oder verweigert werden.

Das folgende Konsolenverfahren und sein AWS CLI Äquivalent zeigen ein Beispiel für die Erstellung einer Richtlinienerklärung, die Nachrichten an Ihren Eingangsendpunkt zulässt, wenn sich der Empfänger in der angegebenen Adressliste befindet.

So verwenden Sie eine Adressliste in einer Erklärung zur Verkehrsrichtlinie:

1. Erstellen Sie eine neue Verkehrsrichtlinie oder bearbeiten Sie eine bestehende, wie unter beschrieben Erstellung von Verkehrsrichtlinien und Richtlinienerklärungen (Konsole)
2. Wählen Sie im Container mit den Richtlinien die Option Zulassen aus, damit die Aktion ausgeführt wird, wenn die Bedingungen der Erklärung erfüllt sind.
3. Erstellen Sie die Bedingung der Anweisung wie folgt:
   - Wählen Sie die Empfängeradresse für das Feld Protokoll aus.
   - Wählen Sie für das Feld Operator die Option Ist in der Adressliste.
   - Wählen Sie den Namen Ihrer Adressliste für das Feld Wert aus.
4. Dies ist zwar nur ein Beispiel, Sie können jedoch weitere Richtlinienbedingungen hinzufügen, die auf einer Vielzahl von Operatoren für jede Ihrer Adresslisten basieren können.

Mit dem AWS CLI:

```
aws mailmanager create-traffic-policy \
  --default-action ALLOW \
  --traffic-policy-name "testpolicy" \
  --policy-statements '[{
    "Action": "ALLOW",
    "Conditions": [{
      "BooleanExpression": {
        "Evaluate": {
          "IsInAddressList": {
            "Attribute": "RECIPIENT",
            "AddressLists": [
              "arn:aws:ses:eu-west-3:123456789012:mailmanager-address-
list/al-123456789abc"
            ]
          }
        },
        "Operator": "IS_TRUE"
      }
  }]
}]'
```

Verwenden einer Adressliste in einer Regel

Adresslisten können ausgewählt werden, wenn Sie die Bedingung einer Regel erstellen, die in einem Ihrer Regelsätze verwendet wird, um die Aktion der Regel auszulösen.

Die folgende Konsolenprozedur und ihre AWS CLI Entsprechung zeigen ein Beispiel für die Erstellung einer Regel, die die Löschaktion auslöst, wenn sich der Empfänger in der angegebenen Adressliste befindet.

So verwenden Sie eine Adressliste in einer Regelbedingung:

1. Erstellen Sie eine neue Regel oder bearbeiten Sie eine bestehende, wie unter beschrieben Regelsätze und Regeln erstellen (Konsole)
2. Erstellen Sie im Container „Regelbedingungen“ die Bedingung der Regel wie folgt.
   - Wählen Sie im Feld Eigenschaft auswählen die Empfängeradresse aus.
   - Wählen Sie für das Feld Operator auswählen die Option Ist in der Adressliste.
   - Wählen Sie den Namen Ihrer Adressliste für das Feld Wert aus.
3. Wählen Sie im Container Aktionen die Option Neue Aktion hinzufügen und anschließend Aktion löschen aus.
4. Dies ist zwar nur ein Beispiel, aber Sie können weitere Regelbedingungen hinzufügen, die auf einer Vielzahl von Operatoren mit beliebigen Adresslisten basieren können, sodass eine Vielzahl von Aktionen ausgeführt werden können.

Verwenden von AWS CLI:

```
aws mailmanager create-rule-set \
  --rule-set-name "testruleset2" \
  --rules '[{
    "Name": "addresslist",
    "Conditions": [{
      "BooleanExpression": {
        "Evaluate": {
          "IsInAddressList": {
            "Attribute": "RECIPIENT",
            "AddressLists": [
              "arn:aws:ses:us-east-1:123456789012:mailmanager-address-
list/al-123456789abc"
            ]
```

```
          }
        },
        "Operator": "IS_TRUE"
      }
    }],
    "Actions": [{
      "Drop": {}
    }]
  }]'
```

Bewährte Methoden und Überlegungen

- Achten Sie auf die Listengröße — sehr große Listen können sich negativ auf die Leistung auswirken.
- Adresslisten sind kontospezifisch und können nur innerhalb desselben Kontos verwendet werden. AWS
- Verschachtelte Adresslisten werden derzeit nicht unterstützt.
- Pro Region werden maximal 100 Adresslisten unterstützt.
- Pro Adressliste werden maximal 100.000 Adressen unterstützt.

E-Mail-Archivierung

Die E-Mail-Archivierung bietet Ihnen die Möglichkeit, die von Ihnen angegebenen E-Mail-Typen zu archivieren, die an Ihren Eingangsendpunkt gelangen, oder E-Mails, die Sie über einen Konfigurationssatz versenden. Außerdem können Sie Ihre archivierten Nachrichten mithilfe einer Vielzahl erweiterter Suchfilter finden und die Ergebnisse exportieren.

Die E-Mail-Archivierung speichert und schützt Ihre E-Mails, indem sie Daten in einem dauerhaften und sicheren Langzeitspeicher speichert und Ihnen die Möglichkeit bietet, E-Mails schnell zu suchen und zu archivieren. Es ermöglicht eine Vollzeitarchivierung auf Unternehmensebene, ohne die Speicheranforderungen Ihres Postfachservers zu erhöhen.

Ein Archiv kann eine Kombination aus gesendeten und empfangenen E-Mails enthalten:

- Archivierung gesendeter E-Mails — Wenn Sie (ausgehende) E-Mails über einen Konfigurationssatz senden, bei dem die Archivierungsoption aktiviert ist, werden alle mit diesem Konfigurationssatz gesendeten E-Mails in dem von Ihnen angegebenen E-Mail-Archiv archiviert.

- Archivierung empfangener E-Mails — Wenn Ihr Eingangsendpunkt (eingehende) E-Mails empfängt, bestimmt er anhand einer Datenverkehrsrichtlinie, welche E-Mails blockiert oder zugelassen werden sollen. Die E-Mail, die Sie zulassen, wird einem Regelsatz übergeben, der bedingte Regeln anwendet, um die Aktionen auszuführen, die Sie für bestimmte Arten von E-Mails definiert haben. Eine der Regelaktionen, die Sie definieren können, ist die Aktion Archivieren. Wenn Sie diese Aktion auswählen, wird die E-Mail in dem von Ihnen angegebenen E-Mail-Archiv archiviert.

Sie müssen zuerst ein Archiv erstellen, bevor es in einer Regelaktion oder einem Konfigurationssatz angegeben werden kann. Das Verfahren im nächsten Abschnitt führt Sie durch die Erstellung eines Archivs in der SES-Konsole.

E-Mail-Archivierung in der Amazon SES SES-Konsole verwenden

Die E-Mail-Archivierungsseite in der SES-Konsole besteht aus den vier interaktiven Tabellen Archiv durchsuchen, Suchverlauf, Exportverlauf und Archive verwalten, mit denen Sie in Ihren Archiven nach E-Mails suchen, die Ergebnisse exportieren und Ihre Archive verwalten können. In den folgenden Verfahren werden Anweisungen für jede Tabelle bereitgestellt.

So verwenden Sie die Seite E-Mail-Archivierung zum Suchen, Exportieren und Verwalten Ihrer Archive

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Mail Manager die Option E-Mail-Archivierung aus.
3. Die Seite E-Mail-Archivierung besteht aus vier Tabellen „Archiv durchsuchen“, „Suchverlauf“, „Exportverlauf“ und „Archive verwalten“. Spezifische Anweisungen für jede dieser Tabellen finden Sie auf der entsprechenden Registerkarte unten:

Search archive

Das Sucharchiv ist eine interaktive Tabelle, mit der Sie Ihre archivierten Nachrichten suchen und finden können. Sie verfügt über umfangreiche Filter und Datumsangaben, anhand derer Sie alles finden können, von einer bestimmten E-Mail bis hin zu vielen E-Mails, die einer breiteren Kategorie entsprechen. Nachrichten, die Ihren Suchkriterien entsprechen, können einzeln heruntergeladen oder in großen Mengen in einen S3-Bucket exportiert werden.

Um archivierte E-Mails zu suchen, herunterzuladen oder zu exportieren

1. Wählen Sie auf der Seite E-Mail-Archivierung die Registerkarte Archiv durchsuchen, um die Tabelle Sucharchiv anzuzeigen.
2. Klicken Sie in das Feld Archiv und wählen Sie ein Archiv aus der Liste, gefolgt von Suchen, oder verfeinern Sie Ihre Suche mithilfe der folgenden Schritte.
3. Wählen Sie das Feld Datumsbereich aus, um die Datumsbereichsoptionen für Ihre Suche zu erweitern:

   - Relativer Bereich (Standard) — Wählen Sie das Optionsfeld aus, das der gewünschten Anzahl von Tagen entspricht, oder wählen Sie einen benutzerdefinierten Bereich aus, indem Sie eine Zeiteinheit und einen Datumsbereich bis zu 30 Tagen auswählen.
   - Absoluter Bereich — Geben Sie ein Start - und ein Enddatum (und eine Uhrzeit, falls gewünscht) bis zu 30 Tagen ein.

   > **Note**
   >
   > - Die Suche in einem Archiv ist auf jeweils 30 Tage begrenzt. Wenn Sie beispielsweise nach Nachrichten vom 1. Juni bis 31. Juli suchen möchten, müssten Sie die Suche wie folgt in drei Suchvorgänge aufteilen:
   >
   >   1. 30 Tage im Juni.
   >   2. Die ersten 30 Tage im Juli.
   >   3. Der 31. Tag im Juli.
   >
   > - Bei Datumsangaben mit relativer Zeitspanne endet der letzte Tag um Mitternacht. Wenn Sie beispielsweise Letzte 7 Tage auswählen, wäre der siebte Tag gestern mit einem Ende um Mitternacht.

4. (Optional) Wählen Sie das Feld Filter aus, um aus den folgenden Filtern auszuwählen: Von, An, CC, Betreffzeile und Hat Anlagen. Dabei gelten die folgenden Eigenschaften:

   - Sie können bis zu 10 Filter erstellen.
   - Ein Filter kann bearbeitet werden, indem Sie darauf klicken, oder Sie können ihn entfernen, indem Sie das X auswählen.

5. Wählen Sie Suchen und die archivierte E-Mail, die Ihren Suchkriterien entspricht, wird in der Tabelle mit den Suchergebnissen angezeigt.

- Die Spalte Nachrichten-ID ist standardmäßig ausgeblendet, kann aber angezeigt werden, indem Sie auf das Zahnradsymbol klicken, um die Ansicht der Tabelle anzupassen.
- Jede von Ihnen ausgeführte Suche wird automatisch mit einer eindeutigen Such-ID gespeichert und in der Tabelle Suchverlauf aufgeführt.

6. Um den Text einer Nachricht zusammen mit ihren Umschlag- und Kopfzeileninformationen anzuzeigen, wählen Sie das Optionsfeld der Nachricht und anschließend Details anzeigen aus, um die Seitenleiste mit den Nachrichtendetails zu öffnen.
7. Um eine lokale Datei der Nachricht zu erstellen, wählen Sie das Optionsfeld der Nachricht und anschließend Nachricht herunterladen aus.
8. Ihre gefilterte Suche kann in einem Amazon S3 S3-Bucket gespeichert werden, indem Sie In S3 exportieren auswählen.

   a. Wenn Sie den URI des S3-Buckets kennen, den Sie verwenden möchten, geben Sie ihn in das Feld S3-URI ein. Andernfalls wählen Sie Browse S3 und wählen Sie einen S3-Bucket und einen S3-Ordner aus, die auf der S3-Seite verwendet werden sollen.

   b. (Optional) Sie können Ihre exportierten Nachrichten verschlüsseln, indem Sie entweder Ihren eigenen AWS KMS Schlüssel in das ARN-Feld KMS-Schlüssel eingeben oder indem Sie Neuen Schlüssel erstellen auswählen. Andernfalls wird für die Verschlüsselung die Methode festgelegt, die für den Ziel-S3-Bucket verwendet wird (auch wenn keine Methode verwendet wird).

   c. Wählen Sie Exportieren und alle Nachrichten, die Sie bei Ihrer gefilterten Suche gefunden haben, werden als einzelne Dateien im ausgewählten S3-Ordner gespeichert.

> **Note**
>
> Es gibt zwar keine Begrenzung, wie viele Nachrichten Ihr Archiv enthalten kann, aber die Suchergebnisse sind in der Tabelle mit den Suchergebnissen auf 1000 Zeilen begrenzt.

Search history

In dieser Tabelle ist ein Verlauf Ihrer Suchanfragen aufgeführt, sodass Sie den Ergebnissatz wiederherstellen oder auf komplexe Filtersätze zugreifen können, die zuvor erstellt wurden. Sie können auch neue Suchen auf der Grundlage der ursprünglichen Suche erstellen, indem Sie die

Filter und Daten bearbeiten. Alle neuen Suchanfragen werden automatisch mit einer eindeutigen Such-ID gespeichert und in dieser Tabelle aufgeführt.

Um Ihre vorherigen Suchanfragen anzusehen und mit ihnen zu arbeiten

1. Wählen Sie auf der Seite E-Mail-Archivierung die Registerkarte Suchverlauf aus, um die Tabelle Suchverlauf anzuzeigen, in der ein Verlauf all Ihrer archivierten E-Mail-Suchanfragen aufgeführt ist, wobei die neuesten ganz oben aufgeführt sind. Diese Tabelle lädt Daten, wenn Sie sie zum ersten Mal aufrufen. Wenn Sie die Tabs wechseln und zurückkehren, verwenden Sie das Aktualisierungssymbol, um die neuesten Daten abzurufen.
2. Klicken Sie in das Feld Archiv und wählen Sie ein Archiv aus der Liste aus. Alle Suchvorgänge, die zu diesem Archiv gehören, werden in die Tabelle übernommen. In den folgenden Schritten können Sie einzelne Suchanfragen ansehen und weitere Aktionen ausführen.
3. Wählen Sie das Optionsfeld einer vorherigen Suche, gefolgt von Suchergebnisse anzeigen, um die ursprünglichen Suchergebnisse wiederherzustellen. Die Seite mit dem Sucharchiv wird geöffnet, auf der der für die ursprüngliche Suche verwendete Filtersatz und der Datumsbereich sowie alle Nachrichten angezeigt werden, die zuvor anhand dieser Kriterien gefunden wurden. Sie können die ursprüngliche Suche auf folgende Weise erweitern:

   - Erstellen Sie eine neue Suche, indem Sie den Datumsbereich und die Filter, gefolgt von Suchen, ändern.
   - Alle neuen Suchvorgänge, die Sie durchführen, werden automatisch mit einer eindeutigen Such-ID gespeichert und in der Tabelle Suchverlauf aufgeführt.

Export history

In dieser Tabelle ist ein Verlauf Ihrer Exporte aufgeführt, sodass Sie in der S3-Konsole einfach auf den Inhalt des Exportordners zugreifen können.

Um Ihre letzten Exporte anzusehen

1. Wählen Sie auf der Seite E-Mail-Archivierung die Registerkarte Exportverlauf aus, um die Tabelle Exportverlauf anzuzeigen, in der alle archivierten E-Mail-Suchanfragen aufgeführt sind, die Sie in den letzten 30 Tagen in einen S3-Bucket exportiert haben. Diese Tabelle lädt Daten, wenn Sie sie zum ersten Mal aufrufen. Wenn Sie die Tabs wechseln und zurückkehren, verwenden Sie das Aktualisierungssymbol, um die neuesten Daten abzurufen.

2. Wenn der Status eines Exports in Warteschlange, Vorverarbeitung oder Verarbeitung lautet, können Sie ihn abbrechen, indem Sie Abbrechen wählen.
3. Wählen Sie eine S3-URI aus, um den Bucket-Ordner des Exports in der S3-Konsole zu öffnen, wo Sie die darin enthaltenen Dateien sehen können.

Manage archives

In dieser Tabelle sind Ihre Archive aufgeführt. Sie haben die Möglichkeit, ein neues Archiv zu erstellen, nach einem bestimmten Archiv zu suchen und dessen Details anzuzeigen, ein Archiv zu bearbeiten oder ein Archiv zu löschen.

Um Archive zu erstellen und zu verwalten

1. Wählen Sie auf der Seite E-Mail-Archivierung die Registerkarte Archive verwalten, um die Tabelle Archive anzuzeigen, in der alle Ihre E-Mail-Archive aufgeführt sind. Diese Tabelle lädt Daten, wenn Sie sie zum ersten Mal aufrufen. Wenn Sie die Tabs wechseln und zurückkehren, verwenden Sie das Aktualisierungssymbol, um die neuesten Daten abzurufen.
2. Um nach einem bestimmten Archiv zu suchen, beginnen Sie mit der Eingabe in das Feld Archiv.
3. Um Details zu einem Archiv anzuzeigen, wählen Sie seinen Namen in der Spalte Archivname aus.
4. Um ein Archiv zu erstellen, wählen Sie Archiv erstellen aus.

    a. Geben Sie einen eindeutigen Namen in das Feld Archivname ein.

    b. (Optional) Wählen Sie im Feld Aufbewahrungszeitraum einen Aufbewahrungszeitraum aus, um den standardmäßigen Aufbewahrungszeitraum von 180 Tagen zu überschreiben.

    c. (Optional) Sie können Ihr Archiv verschlüsseln, indem Sie entweder Ihren eigenen AWS KMS Schlüssel in das Feld KMS-Schlüssel ARN eingeben oder indem Sie Neuen Schlüssel erstellen auswählen.

    Wählen Sie Archiv erstellen.
5. Nachdem Sie ein Archiv erstellt haben, können Sie es in einem Regelsatz verwenden, um empfangene (eingehende) E-Mails zu archivieren, oder es in einem Konfigurationssatz für die Archivierung gesendeter (ausgehender) E-Mails festlegen.

6. Um ein Archiv zu bearbeiten, wählen Sie das entsprechende Optionsfeld und anschließend Bearbeiten aus.

   a. Bearbeiten oder ändern Sie den Namen im Feld Archivname.

   b. Ändern Sie den Aufbewahrungszeitraum im Feld Aufbewahrungszeitraum.

   Wählen Sie Archiv aktualisieren.

7. Um ein Archiv zu löschen, wählen Sie das entsprechende Optionsfeld und anschließend Löschen aus.

   - Geben Sie das **`delete`** Feld Bestätigen gefolgt von Löschen ein.

     Der Archivstatus wechselt in der Tabelle Archive auf Ausstehende Löschung und wird nach 30 Tagen automatisch gelöscht.

E-Mail-Add-Ons

Email Add Ons ist eine Sammlung spezialisierter Sicherheitstools von von von SES zugelassenen Anbietern, mit denen Sie die Art von E-Mail verwalten können, die Sie für Ihren Eingangsendpunkt zulassen, und um festzulegen, welche Maßnahmen für bestimmte Arten von E-Mails ergriffen werden sollen. Bei diesen Tools handelt es sich um zertifizierte Lösungen für Sicherheitsinformationen und -durchsetzung, die sofort in Ihren E-Mail-Workflow integriert werden können und direkt über die Mail Manager-Konsole aktiviert werden können.

Diese Add-Ons bieten die Flexibilität, zwischen geprüften E-Mail-Sicherheitslösungen zu wählen, die für Ihre individuellen Anwendungsfälle geeignet sind und zu einem bestimmten Preis verwendet werden können, anstatt eine große, einzelne Produktlösung zu kaufen, die möglicherweise nicht für Ihre Anforderungen optimiert ist. Email Add Ons erweitert seine Kernfunktionen für Bedrohungsinformationen und Sicherheitsdurchsetzung auf Workload-Basis, sodass Sie sich keine Gedanken über die benötigte Kapazität machen müssen. Dank dieser Vorteile können Sie sich darauf konzentrieren, E-Mail-Sicherheitsproblemen immer einen Schritt voraus zu sein und hohe Servicestandards für Ihr Unternehmen aufrechtzuerhalten.

Weitere Informationen zu den einzelnen Add-Ons finden Sie direkt auf der Seite E-Mail-Add-Ons in der Mail Manager-Konsole. Dort haben Sie Zugriff auf Produktbeschreibungen, Hauptvorteile und Preisinformationen. Sobald Sie sich für ein Add-On entschieden haben, das Sie verwenden möchten, abonnieren Sie es einfach über die Mail Manager-Konsole. Sobald Sie das Abonnement

abgeschlossen haben, können Sie es als Bedingung für die Datenverkehrsrichtlinie auswählen, um festzulegen, welche E-Mails an einem Eingangsendpunkt zugelassen sind, oder als Regelsatzbedingung, um festzulegen, welche Aktionen für bestimmte E-Mails ergriffen werden sollen. Die primäre Unterstützung für alle Add-Ons wird von der Mail Manager-Konsole bereitgestellt AWS und kann auch von dort aus aufgerufen werden.

Das Verfahren im nächsten Abschnitt führt Sie durch das Abonnieren eines E-Mail-Add-Ons in der Mail Manager-Konsole.

Abonnieren von E-Mail-Add-Ons in der Mail Manager-Konsole

Das folgende Verfahren zeigt Ihnen, wie Sie die Seite „E-Mail-Add-Ons“ in der Mail Manager-Konsole verwenden, um ein Add On zu abonnieren, sodass es in allen Ihren Verkehrsrichtlinien oder Regelsätzen verwendet werden kann.

So abonnieren Sie ein E-Mail-Add-On über die Konsole

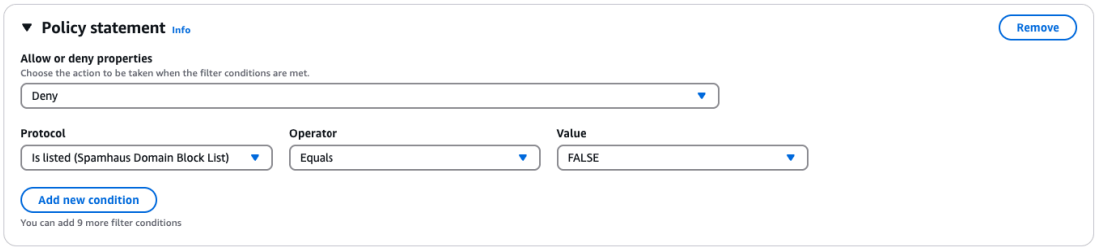
1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im linken Navigationsbereich unter Mail Manager die Option E-Mail-Add-Ons aus.
3. Wählen Sie auf der Seite „E-Mail-Add-Ons“ den Titel einer beliebigen Zusatzkarte aus, um deren Übersichtsseite zu öffnen. Dort erfahren Sie mehr über ihre Funktionen, ihre wichtigsten Vorteile und Preisinformationen. Wenn Sie dieses Add-On verwenden möchten, wählen Sie Abonnieren.

   - Lesen Sie die angezeigten Allgemeinen Geschäftsbedingungen und aktivieren Sie das Kontrollkästchen Ich akzeptiere, gefolgt von Abonnieren.
4. Sobald Sie ein Add-On abonniert haben, können Sie es in Ihren E-Mail-Workflow integrieren, indem Sie es als Verkehrsrichtlinienbedingung auswählen, um E-Mails an Ihren Eingangsendpunkt zu verweigern oder zuzulassen, oder als regelfestgelegte Bedingung, um festzulegen, welche Aktion bei qualifizierten Nachrichten ergriffen werden soll.

   Die folgenden Beispiele zeigen die Verwendung eines Add-Ons in einer Grundsatzerklärung und in einer Regelbedingung:

   Beispiel für eine Verkehrsrichtlinie mit einem Add-On

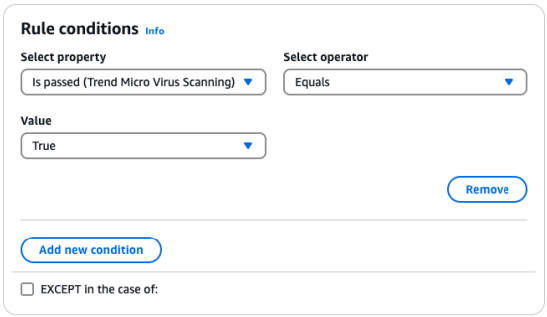
   Verwenden Sie das Add-On „Spamhaus Domain Block List“ in einer Grundsatzerklärung, um E-Mails zu blockieren, die von einer in Spamhaus gelisteten Domain stammen:



Einzelheiten zur Erstellung von Richtlinien für den Datenverkehr und zur Erstellung von Richtlinien-Bedingungen mit E-Mail-Add-Ons finden Sie unter. the section called “Erstellung von Verkehrsrichtlinien und Richtlinienerklärungen (Konsole)”

Beispiel für eine Regelbedingung mit einem Add-On

Verwenden Sie das Trend Micro Virus Scanning Add-On in einer Regelbedingung, um eine Regelaktion für E-Mails zu bestimmen, die den Virenscan bestehen:



Einzelheiten zur Erstellung von Regelsätzen und zur Erstellung von Regelbedingungen mit E-Mail-Add-Ons finden Sie unterthe section called “Regelsätze und Regeln erstellen (Konsole)”.

5. Um allgemeine Informationen oder Support für ein von Ihnen abonniertes Add-On einzusehen oder auf Support zuzugreifen, wählen Sie den entsprechenden Namen auf der Seite „E-Mail-Add-Ons“ aus, um die entsprechende Übersichtsseite zu öffnen:

   - Unter Allgemeine Informationen können Sie das Datum Ihres Abonnements und den Amazon-Ressourcennamen (ARN) Ihres Add-Ons einsehen.
   - Wählen Sie die Registerkarte Support, um auf Links zum AWS Support zuzugreifen.

6. Um sich von einem Add-On abzumelden:

   a. Sie müssen es zunächst aus Ihren Verkehrsrichtlinien oder Regelsätzen entfernen, in denen Sie es in einer Bedingung definiert haben. Andernfalls schlagen die folgenden Schritte zum Abbestellen fehl.

b. Wählen Sie den Namen auf der Seite E-Mail-Add-Ons aus, um die zugehörige Übersichtsseite zu öffnen, gefolgt von Abbestellen.

c. Geben Sie das **`confirm`** Feld Bestätigen gefolgt von Abbestellen ein.

Berechtigungsrichtlinien für Mail Manager

Die Richtlinien in diesem Kapitel dienen als zentrale Referenz für die Richtlinien, die zur Nutzung der verschiedenen Funktionen von Mail Manager erforderlich sind.

Auf den Seiten mit den Funktionen von Mail Manager finden Sie Links, über die Sie zu dem entsprechenden Abschnitt auf dieser Seite gelangen, der die Richtlinien enthält, die Sie für die Nutzung der Funktion benötigen. Wählen Sie das Symbol zum Kopieren der gewünschten Richtlinie aus und fügen Sie es wie in der Beschreibung der jeweiligen Funktion beschrieben ein.

Die folgenden Richtlinien geben Ihnen die Erlaubnis, die verschiedenen Funktionen von Amazon SES Mail Manager mithilfe von Richtlinien und AWS Secrets Manager Richtlinien für Ressourcenberechtigungen zu nutzen. Wenn Sie mit den Genehmigungsrichtlinien noch nicht vertraut sind, finden Sie the section called “Richtlinienanatomie” weitere Informationen unter Genehmigungsrichtlinien für AWS Secrets Manager.

Berechtigungsrichtlinien für den Ingress-Endpunkt

Beide Richtlinien in diesem Abschnitt sind erforderlich, um einen Eingangsendpunkt zu erstellen. Informationen zum Erstellen eines Eingangsendpunkts und zur Verwendung dieser Richtlinien finden Sie unter. the section called “Einen Ingress-Endpunkt (Konsole) erstellen”

Secrets Manager Secrets-Ressourcenberechtigungsrichtlinie für Eingangsendpunkte

Die folgende Secrets Manager Manager-Ressourcenberechtigungsrichtlinie ist erforderlich, damit SES über die Eingangsendpunktressource auf das Secret zugreifen kann.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "Id",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "000000000000"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ses:us-
east-1:000000000000:mailmanager-ingress-point/*"
                }
            }
        }
    ]
}
```

KMS-Schlüsselrichtlinie für vom Kunden verwaltete Schlüssel (CMK) für den Eingangsendpunkt

Es ist erforderlich, einen vom Kunden verwalteten Schlüssel (CMK) für Ihr Geheimnis zu verwenden. Die folgende Erklärung ist in Ihrer KMS-Schlüsselrichtlinie erforderlich, damit SES Ihren Schlüssel für Ihr Geheimnis verwenden kann.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ses.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "secretsmanager.us-east-1.amazonaws.com",
            "aws:SourceAccount": "000000000000"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:ses:us-east-1:000000000000:mailmanager-ingress-
point/*"
        }
```

```
    }
}
```

KMS-Schlüsselrichtlinie für vom Kunden verwaltete Schlüssel (CMK) für den MTLs Trust Store

Wenn Sie einen vom Kunden verwalteten Schlüssel (CMK) verwenden, um Ihren mTLS Trust Store zu verschlüsseln, ist die folgende Aussage in Ihrer KMS-Schlüsselrichtlinie erforderlich, damit SES Ihren Schlüssel verwenden kann.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ses.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "000000000000"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:ses:us-east-1:000000000000:mailmanager-ingress-
point/*"
        }
    }
}
```

Berechtigungsrichtlinien für SMTP-Relay

Beide Richtlinien in diesem Abschnitt sind erforderlich, um ein SMTP-Relay zu erstellen. Informationen zum Erstellen eines SMTP-Relays und zur Verwendung dieser Richtlinien finden Sie unter. the section called “Ein SMTP-Relay (Konsole) erstellen”

Secrets Manager Secrets-Ressourcenberechtigungsrichtlinie für SMTP-Relay

Die folgende Secrets Manager Manager-Ressourcenberechtigungsrichtlinie ist erforderlich, damit SES über die SMTP-Relay-Ressource auf das Secret zugreifen kann.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Principal": {
                "Service": [
                    "ses.amazonaws.com"
                ]
            },
            "Resource": "*",
            "Condition": {
               "StringEquals": {
                   "aws:SourceAccount": "888888888888"
                },
               "ArnLike": {
                   "aws:SourceArn": "arn:aws:ses:us-
east-1:888888888888:mailmanager-smtp-relay/*"
                }
           }
        }
    ]
}
```

KMS-Schlüsselrichtlinie für vom Kunden verwaltete Schlüssel (CMK) für SMTP-Relay

Die folgende Erklärung ist in Ihrer KMS-Schlüsselrichtlinie erforderlich, damit SES Ihren Schlüssel für Ihr Geheimnis verwenden kann.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.us-east-1.amazonaws.com",
                    "aws:SourceAccount": "000000000000"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ses:us-
east-1:000000000000:mailmanager-smtp-relay/*"
                }
            }
        }
    ]
}
```

Berechtigungsrichtlinien für die E-Mail-Archivierung

Archivierung, Export.

Der IAM-Identitätsaufruf `StartArchiveExport` muss Zugriff auf den Ziel-S3-Bucket haben, der gemäß der folgenden IAM-Richtlinie konfiguriert wurde:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
```

```
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
        }
    ]
}
```

Dies ist die S3-Bucket-Richtlinie für den Ziel-Bucket:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
```

```
                "s3:PutObjectTagging",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
        }
    ]
}
```

> **Note**
>
> Die Archivierung unterstützt keine konfusen stellvertretenden Bedingungsschlüssel (aws: SourceArnSourceAccount, aws:, aws: SourceOrg ID oder aws:SourceOrgPaths). Das liegt daran, dass die E-Mail-Archivierung von Mail Manager das Problem mit verwirrten Stellvertretern verhindert, indem sie anhand von Forward Access Sessions testet, ob die aufrufende Identität über Schreibberechtigungen für den Exportziel-Bucket verfügt, bevor der eigentliche Export gestartet wird.

Archivierung (Verschlüsselung im Ruhezustand) mit KMS CMK

Die IAM-Identität ruft an `CreateArchive` und `UpdateArchive` muss über die folgende Richtlinie Zugriff auf den KMS-Schlüssel-ARN haben:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "kms:DescribeKey",
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:us-east-1:111122223333:key/MyKmsKeyArnID"
    }
}
```

Die folgenden Aussagen sind in Ihrer KMS-Schlüsselrichtlinie erforderlich:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/MyUserRoleOrGroupName"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": [
                        "ses.us-east-1.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Berechtigungs- und Vertrauensrichtlinien für die Ausführung von Regelaktionen

Die SES-Regelausführungsrolle ist eine AWS Identity and Access Management (IAM) -Rolle, die den Regeln Ausführungsberechtigungen für den Zugriff auf AWS Dienste und Ressourcen erteilt. Bevor Sie eine Regel in einem Regelsatz erstellen, müssen Sie eine IAM-Rolle mit einer Richtlinie erstellen, die den Zugriff auf die erforderlichen AWS Ressourcen ermöglicht. SES übernimmt diese Rolle bei der Ausführung einer Regelaktion. Sie könnten beispielsweise eine Rolle zur Ausführung von Regeln erstellen, die berechtigt ist, eine E-Mail-Nachricht als Regelaktion in einen S3-Bucket zu schreiben, die dann ausgeführt werden kann, wenn die Bedingungen Ihrer Regel erfüllt sind.

Daher ist zusätzlich zu den individuellen Berechtigungsrichtlinien in diesem Abschnitt, die für die Ausführung der einzelnen Regelaktionen erforderlich sind, die folgende Vertrauensrichtlinie erforderlich.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "ses.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
          "StringEquals": {
                   "aws:SourceAccount": "888888888888"
          },
          "ArnLike": {
             "aws:SourceArn": "arn:aws:ses:us-east-1:888888888888:mailmanager-
rule-set/*"
          }
        }
      }
    ]
  }
```

Richtlinien für Regelaktionen

- Berechtigungsrichtlinie für die Regelaktion „In S3 schreiben“
- Berechtigungsrichtlinie für die Regelaktion „An Postfach senden“
- Berechtigungsrichtlinie für die Regelaktion „An Internet senden“
- Berechtigungsrichtlinie für die Regelaktion „An ein Unternehmen liefern“
- Berechtigungsrichtlinie für die Regelaktion „In SNS veröffentlichen“
- Berechtigungsrichtlinie für die Aktion „Bounce-Regel“
- Berechtigungsrichtlinie für die Regelaktion „Lambda-Funktion aufrufen“

Berechtigungsrichtlinie für die Regelaktion „In S3 schreiben“

Die folgende Richtlinie ist erforderlich, damit Ihre IAM-Rolle die Regelaktion „In S3 schreiben“ verwendet, mit der die empfangene E-Mail an einen S3-Bucket weitergeleitet wird.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutObject",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::MyDestinationBucketName/*"
            ]
        },
        {
            "Sid": "AllowListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::MyDestinationBucketName"
            ]
```

```
        }
    ]
}
```

Wenn Sie den vom AWS KMS Kunden verwalteten Schlüssel für einen S3-Bucket mit aktivierter serverseitiger Verschlüsselung verwenden, müssen Sie die IAM-Rollenrichtlinien-Aktion hinzufügen,. `"kms:GenerateDataKey*"` Im vorherigen Beispiel würde das Hinzufügen dieser Aktion zu Ihrer Rollenrichtlinie wie folgt aussehen:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowKMSKeyAccess",
            "Effect": "Allow",
            "Action": "kms:GenerateDataKey*",
            "Resource": "arn:aws:kms:us-east-1:888888888888:key/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "kms:ResourceAliases": [
                        "alias/MyKeyAlias"
                    ]
                }
            }
        }
    ]
}
```

Weitere Informationen zum Anhängen von Richtlinien an AWS KMS Schlüssel finden Sie unter Verwenden von Schlüsselrichtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Berechtigungsrichtlinie für die Regelaktion „An Postfach senden“

Die folgende Richtlinie ist erforderlich, damit Ihre IAM-Rolle die Regelaktion „An Postfach versenden“ verwendet, mit der die empfangene E-Mail an ein WorkMail Amazon-Konto zugestellt wird.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["workmail:DeliverToMailbox"],
        "Resource": "arn:aws:workmail:us-
east-1:888888888888:organization/MyWorkMailOrganizationID>"
      }
    ]
  }
```

Berechtigungsrichtlinie für die Regelaktion „An Internet senden“

Die folgende Richtlinie ist erforderlich, damit Ihre IAM-Rolle die Regelaktion „An Internet senden“ verwendet, mit der die empfangene E-Mail an eine externe Domain gesendet wird.

> **Note**
>
> Wenn Ihre SES-Identität einen Standardkonfigurationssatz verwendet, müssen Sie auch die Konfigurationssatz-Ressource hinzufügen, wie im folgenden Beispiel gezeigt.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["ses:SendEmail", "ses:SendRawEmail"],
        "Resource":[
        "arn:aws:ses:us-east-1:888888888888:identity/example.com",
        "arn:aws:ses:us-east-1:888888888888:configuration-set/my-configuration-
set"
        ]
      }
```

```
    ]
  }
```

Berechtigungsrichtlinie für die Regelaktion „An ein Unternehmen liefern“

Die folgenden Richtlinien sind erforderlich, um die Regelaktion „An Q Business versenden“ zu verwenden, mit der die empfangene E-Mail an einen Amazon Q Business-Index weitergeleitet wird.

Für Ihre Rolle ist eine IAM-Richtlinie erforderlich:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessToQBusiness",
            "Effect": "Allow",
            "Action": [
                "qbusiness:BatchPutDocument"
            ],
            "Resource": [
                "arn:aws:qbusiness:us-
east-1:888888888888:application/ApplicationID/index/IndexID"
            ]
        }
    ]
}
```

In Ihrer KMS-Schlüsselrichtlinie ist eine Erklärung erforderlich:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessToKMSKeyForQbusiness",
            "Effect": "Allow",
```

```
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Encrypt",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:888888888888:key/*"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "qbusiness.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "888888888888"
                 },
                 "ForAnyValue:StringEquals": {
                    "kms:ResourceAliases": [
                        "alias/MyKeyAlias"
                    ]
                }
            }
        }
    ]
}
```

Weitere Informationen zum Anhängen von Richtlinien an AWS KMS Schlüssel finden Sie unter Verwenden von Schlüsselrichtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Berechtigungsrichtlinie für die Regelaktion „In SNS veröffentlichen“

Die folgenden Richtlinien sind erforderlich, um die Regelaktion „In SNS veröffentlichen“ zu verwenden, mit der die empfangene E-Mail an ein Amazon SNS-Thema weitergeleitet wird.

Für Ihre Rolle ist eine IAM-Richtlinie erforderlich:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessToSNSTopic",
```

```
            "Effect": "Allow",
            "Action": [
                "sns:Publish"
            ],
            "Resource": [
                "arn:aws:sns:us-east-1:888888888888:MySnsTopic"
            ]
        }
    ]
}
```

In Ihrer KMS-Schlüsselrichtlinie ist eine Erklärung erforderlich:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessToKMSKeyForSNS",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Encrypt",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:888888888888:key/*"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "qbusiness.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "888888888888"
                 },
                 "ForAnyValue:StringEquals": {
                    "kms:ResourceAliases": [
                        "alias/MyKeyAlias"
                    ]
                }
            }
        }
    ]
```

```
}
```

Weitere Informationen zum Anhängen von Richtlinien an AWS KMS Schlüssel finden Sie unter Verwenden von Schlüsselrichtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

Berechtigungsrichtlinie für die Aktion „Bounce-Regel“

Die folgende Richtlinie ist erforderlich, damit Ihre IAM-Rolle die Aktion „Bounce-Regel“ verwenden kann, bei der die E-Mail zurückgesendet wird, indem sie eine Bounce-Antwort an den Absender zurücksendet.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSendBounce",
            "Effect": "Allow",
            "Action": [
                "ses:SendBounce"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:123456789012:identity/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ses:FromAddress": "sender@example.com"
                }
            }
        }
    ]
}
```

Berechtigungsrichtlinie für die Regelaktion „Lambda-Funktion aufrufen“

Die folgende Richtlinie ist erforderlich, damit Ihre IAM-Rolle die Regelaktion „Lambda-Funktion aufrufen“ verwendet, die eine AWS Lambda Funktion zur Verarbeitung der E-Mail aufruft.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowInvokeLambdaFunction",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:us-east-1:123456789012:function:MyFunction"
            ]
        }
    ]
}
```

Mail Manager-Protokollierung

Die Mail Manager-Protokollierung bietet einen detaillierten Einblick in Ihre Mail Manager-Vorgänge. Die Protokollierungsfunktion verfolgt den Nachrichtenfluss vom ersten Empfang an Eingangsendpunkten bis hin zur Nachrichtenverarbeitung auf der Grundlage Ihrer konfigurierten Regelsätze und Regeln.

Mail Manager bietet Protokollierung für die folgenden Ressourcen:

- Eingangsendpunkte
- Regelsätze

Mail Manager übermittelt Protokolle mithilfe des Amazon CloudWatch Logs-Service. Die Protokolle können an jedes der folgenden Ziele gesendet werden: CloudWatch Logs, Amazon S3 oder Amazon Data Firehose.

Einrichtung der Mail Manager-Protokollzustellung

Eine funktionierende Protokollzustellung besteht aus drei Elementen:

- DeliverySource— Ein logisches Objekt, das die Ressource darstellt, die die Protokolle sendet — entweder einen Eingangsendpunkt oder einen Regelsatz.
- DeliveryDestination— Ein logisches Objekt, das das tatsächliche Lieferziel darstellt (CloudWatch Logs, S3 oder Firehose).
- Lieferung — Verbindet eine Zustellungsquelle mit einem Lieferziel.

In diesem Abschnitt wird erklärt, wie Sie diese Objekte erstellen und welche Berechtigungen für die Verwendung der Mail Manager-Protokollierung erforderlich sind.

Voraussetzungen

Bevor Sie die Mail Manager-Protokollierung einrichten, stellen Sie sicher, dass:

1. Sie haben entweder einen Ingress-Endpunkt oder einen Regelsatz erstellt.
2. Sie verfügen über die erforderlichen CloudWatch Logs- und SES Mail Manager-Berechtigungen, um Protokolle von Ihren Mail Manager-Ressourcen an ihre Lieferziele zu versenden.

Erforderliche Berechtigungen

Sie müssen die Berechtigungen für verkaufte Logs einrichten, wie im Abschnitt Protokollierung, für die zusätzliche Berechtigungen erforderlich sind [V2] des Amazon CloudWatch Logs-Benutzerhandbuchs beschrieben, und die Berechtigungen anwenden, die Ihrem Lieferziel entsprechen:

- An Logs gesendete Logs CloudWatch
- An Amazon S3 gesendete Protokolle
- An Firehose gesendete Logs

Darüber hinaus benötigt Mail Manager die folgenden Benutzerberechtigungen, um die Protokollzustellung zu konfigurieren:

- `ses:AllowVendedLogDeliveryForResource`— Erforderlich, damit Mail Manager die Protokolle in Ihrem Namen an CloudWatch Logs für Ihre spezifischen Ressourcen weitergeben kann, wie im Beispiel gezeigt:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSesMailManagerLogDelivery",
            "Effect": "Allow",
```

```
            "Action": [
                "ses:AllowVendedLogDeliveryForResource"
            ],
            "Resource": [
            "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/inp-
xxxxx",
            "arn:aws:ses:us-east-1:111122223333:mailmanager-rule-set/rs-xxxx"
            ]
        }
    ]
}
```

Aktivierung der Protokollierung in der SES-Konsole

Gehen Sie wie folgt vor, um die Protokollierung für Mail Manager-Ressourcen mithilfe der Konsole zu aktivieren:

1. Öffnen Sie die SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Mail Manager entweder Ingress-Endpoints oder Rule Sets aus und wählen Sie die spezifische Ressource aus, die Sie für die Protokollierung aktivieren möchten.
3. Erweitern Sie auf der Detailseite der Ressource die Option Protokollzustellung hinzufügen und wählen Sie Lieferung an CloudWatch Logs, S3 oder Firehose aus.
4. Folgen Sie im Dialogfeld „Versand hinzufügen zu“ für das von Ihnen gewählte Ziel den Anweisungen, um die für den Zieltyp spezifischen Optionen für die Protokollzustellung zu konfigurieren.
5. (Optional) Erweitern Sie Zusätzliche Einstellungen, um die Felder für den Datensatz, das Ausgabeformat, das Feldtrennzeichen und andere für den Zieltyp spezifische Parameter anzupassen.

Aktivieren der Protokollierung mithilfe der CloudWatch Logs-API

Um die Protokollierung für Mail Manager-Ressourcen mithilfe der CloudWatch Logs-API zu aktivieren, müssen Sie:

1. Erstellen Sie eine DeliverySource mit `PutDeliverySource`.
2. Erstelle ein DeliveryDestination mit `PutDeliveryDestination`.

3. Erstellen Sie eine Lieferung, indem Sie genau eine Lieferquelle und ein Lieferziel verknüpfen, indem Sie `CreateDelivery`.

Beispiele für IAM-Rollen- und Berechtigungsrichtlinien mit allen erforderlichen Berechtigungen für Ihr spezifisches Protokollierungsziel finden Sie im Abschnitt Protokollierung, für die zusätzliche Berechtigungen erforderlich sind [V2] des Amazon CloudWatch Logs-Benutzerhandbuchs. Folgen Sie den Beispielen für IAM-Rollen- und Berechtigungsrichtlinien für Ihr Logging-Ziel, einschließlich der Zulassung von Updates für Ihre spezifische Logging-Zielressource wie CloudWatch Logs, S3 oder Firehose.

> **Note**
>
> Bei der Erstellung eines `resourceArn`kann DeliverySource es sich um einen Ingress-Endpunkt-ARN oder einen Regelsatz-ARN ARN. Je nach `logType`kann DeliverySource das wie folgt aussehen:
>
> - Eingangsendpunkt ARN — oder `APPLICATION_LOGS` `TRAFFIC_POLICY_DEBUG_LOGS`
> - Regelsatz ARN — `APPLICATION_LOGS`

Interpretieren der Protokolle

Die Protokolle können verwendet werden, um zusätzliche Einblicke in den Fluss Ihrer empfangenen Nachrichten zu erhalten, während diese von Mail Manager verarbeitet werden.

In den folgenden Beispielen werden die verschiedenen Felder der Protokolle für jede Ressource und jeden Protokolltyp detailliert beschrieben:

Beispiele für Protokolle

- Endpunktprotokolle für eingehende Zugriffe — APPLICATION_LOGS
- Logs von Eingangsendpunkten — TRAFFIC_POLICY_DEBUG_LOGS
- Regelsatzprotokolle — APPLICATION_LOGS

Endpunktprotokolle für eingehende Zugriffe — **`APPLICATION_LOGS`**

Die Protokolle werden pro Nachricht generiert.

```
{
  "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-ingress-point/inp-
xxxxx",
  "event_timestamp": 1728562395042,
  "ingress_point_type": "OPEN" | "AUTH" | "MTLS",
  "ingress_point_name": "MyIngressPoint",
  "message_id": "0000llcki1jmushh817gr586f963a5inhkvnh81",
  "message_size_bytes": 100000,
  "rule_set_id": "rs-xxxx",
  "sender_ip_address": "1.2.3.4",
  "smtp_mail_from": "someone@domain.com",
  "smtp_helo": "domain.com",
  "tls_protocol": "TLSv1.2",
  "tls_cipher_suite": "TLS_AES_256_GCM_SHA384",
  "recipients": ["me@mydomain.com", "you@mydomain.com", "they@mydomain.com"],
  "ingress_point_metadata": {
       // Only applies to AUTH Ingress endpoint
       "password_version": "",
       "secrets_manager_arn": "",
       // Only applies to MTLS Ingress endpoint
       "client_certificate_details": {
           "common_names": ["mail.example.com"],
           "serial_number": "0A:DE:EB:89:42:FB:1C:67",
           "subject_alternative_names": ["mail.example.com", "smtp.example.com"],
           "issuer": "CN=Example CA,O=Example Corp,C=US",
           "not_before": "2025-01-15T00:00:00Z",
           "not_after": "2026-01-15T23:59:59Z"
       },
       "trust_store_monitoring": {
           "ca_invalid_or_near_expiry": [
               {
                   "subject": "CN=Example CA,O=Example Corp,C=US",
                   "not_before": "2023-06-01T00:00:00Z",
                   "not_after": "2025-05-15T23:59:59Z"
               },
               ...
           ],
           "crl_invalid_or_near_expiry": [
               {
                   "issuer": "CN=Example CA,O=Example Corp,C=US",
                   "this_update": "2025-03-01T00:00:00Z",
                   "next_update": "2025-04-01T00:00:00Z"
               },
```

```
                ...
            ]
        }
    }
}
```

> **Note**
>
> Protokolle werden nur für Nachrichten erstellt, die vom Eingangsendpunkt akzeptiert werden. Ein Eingangsendpunkt, der alle eingehenden Nachrichten ablehnt, veröffentlicht keine Anwendungsprotokolle.

> **Note**
>
> Die `trust_store_monitoring` Listen (`ca_invalid_or_near_expiryundcrl_invalid_or_near_expiry`) geben jeweils maximal 10 Einträge zurück. „Beinahe ablaufend“ bedeutet, dass das Zertifikat oder die CRL innerhalb von 90 Tagen abläuft.

Beispiel für CloudWatch Logs Insights-Abfragen

Nachrichten von sender@domain.com abfragen:

```
fields @timestamp, @message, @logStream, @log
| filter smtp_mail_from like /sender@domain.com/
| sort @timestamp desc
| limit 10000
```

Nachrichten mit einer Größe von mehr als 5000 Byte abfragen:

```
fields @timestamp, @message, @logStream, @log
| filter message_size_bytes > 5000
| sort @timestamp desc
| limit 10000
```

Logs von Eingangsendpunkten — **`TRAFFIC_POLICY_DEBUG_LOGS`**

Die Protokolle werden pro Empfänger generiert.

```
{
    "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-ingress-point/inp-
xxxxx",
    "event_timestamp": 1728562395042,
    "ingress_point_type": "OPEN" | "AUTH",
    "ingress_point_id": "inp-xxxx",
    "ingress_point_session_id": "xxxx",
    "traffic_policy_id": "tp-xxxx",
    "traffic_policy_evaluation": [
           // Array of policy evaluations
           {
                "action": "ALLOW" | "DENY",
                "conditions": [
                // Array of conditions
                {
                    "expression": {
                        "attribute": "RECIPIENT",
                        "operator": "CONTAINS",
                        "value": ["@domain.com", "@mydomain.com"]
                    },
                    "expressionResult": true | false
                }],
                "policyStatementMatched": true | false
            },
            // If no policy statement match then default action will be applied
            {
                "action": "ALLOW" | "DENY",
                "policyStatementMatched": true,
                "type": "DefaultAction",
                "scope": "Recipient"
            },
            // Only present if the email was too large according to the traffic policy
            {
                "action": "DENY",
                "allowedMessageSize": 41943040,
                "receivedMessageSize": 42495384,
                "scope": "Data"
            }
    ],
    "traffic_policy_verdict": "REJECT" | "ACCEPT",
    "sender_ip_address": "1.2.3.4",
    "smtp_mail_from": "someone@domain.com",
    "smtp_helo": "domain.com",
```

```
    "tls_protocol": "TLSv1.2",
    "recipient": "me@mydomain.com",
    "tls_cipher_suite": "TLS_AES_256_GCM_SHA384"
}
```

> **Note**
>
> - Protokolle werden für alle Nachrichten erstellt, die anhand der Datenverkehrsrichtlinie am Eingangsendpunkt ausgewertet werden, unabhängig davon, ob sie akzeptiert oder abgelehnt wurden.
> - Alle Bewertungen der Verkehrsrichtlinien der Empfänger, die zu derselben Nachricht gehören (innerhalb derselben SMTP-Konversation), haben dieselbe Gemeinsamkeit. `ingress_point_session_id` Diese ID dient als Korrelations-ID, da sie erst nach der Annahme der Nachricht verfügbar `message_id` ist.
> - Der `traffic_policy_evaluation` Inhalt hängt von Ihrer Konfiguration ab und kann vorzeitig beendet werden, sobald ein Urteil gefällt wurde.

Beispiel: CloudWatch Logs & Insights-Abfragen

Nachrichten von sender@domain.com abfragen:

```
fields @timestamp, @message, @logStream, @log
| filter smtp_mail_from like /sender@domain.com/
| sort @timestamp desc
| limit 10000
```

Nachrichten abfragen, die zu einem bestimmten Thema gehören`ingress_point_session_id`:

```
fields @timestamp, @message, @logStream, @log
| filter ingress_point_session_id = 'xxx'
| sort @timestamp desc
| limit 10000
```

Nachrichten abfragen, die abgelehnt wurden:

```
fields @timestamp, @message, @logStream, @log
| filter traffic_policy_verdict = 'REJECT'
```

```
| sort @timestamp desc
| limit 10000
```

Regelsatzprotokolle — **APPLICATION_LOGS**

Die Protokolle werden pro Nachricht und Aktion generiert. Das bedeutet, dass jedes Mal, wenn eine Nachricht durch eine Aktion in einer Regel im Regelsatz verarbeitet wird, ein Protokolldatensatz generiert wird:

```
{
   "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-rule-set/rs-xxxx",
   "event_timestamp": 1732298258254,
   "message_id": "0000llcki1jmushh817gr586f963a5inhkvnh81",
   "rule_set_name": "MyRuleSet",
   "rule_name": "MyRule",
   "rule_index": 1,
   "recipients_matched": ["recipient1@domain.com", "recipient2@domain.com"],
   "action_metadata": {
       "action_name": "WRITE_TO_S3" | "DROP" | "RELAY" | "DELIVER_TO_MAILBOX" | etc.,
       "action_index": 2,
       "action_status": "SUCCESS" | "FAILURE" | "IN_PROGRESS",
       "action_failure": "Access denied"
   }
}
```

- `recipients_matched`— Die Empfänger, auf die die Bedingungen der Regel zutreffen, für die die Aktion ausgeführt wird.
- `rule_index`— Die Reihenfolge der Regel innerhalb des Regelsatzes.
- `action_index`— Die Reihenfolge der Aktion innerhalb der Regel.
- `action_status`— Zeigt das Ergebnis der Ausführung der Aktion für die angegebene Nachricht an.
- `action_failure`— Zeigt die Fehlerdetails der Aktion an (gilt nur, wenn eine Aktion fehlschlägt). Zum Beispiel, wenn die angegebene Rolle nicht über genügend Berechtigungen verfügt, um die Aktion auszuführen.

Wenn die Regelbedingungen für eine Nachricht nicht zutreffen, d. h. wenn die Nachricht nicht von der Regel verarbeitet wird, wird außerdem ein einzelnes Protokoll veröffentlicht, das angibt, dass die Nachricht nach dem Regelsatz verarbeitet wurde, aber keine Aktionen darauf ausgeführt wurden:

```
{
   "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-rule-set/rs-xxxx",
   "event_timestamp": 1732298258254,
   "message_id": "0000llcki1jmushh817gr586f963a5inhkvnh81",
   "rule_set_name": "MyRuleSet",
   "rule_name": "MyRule",
   "rule_index": 1,
   "recipients_matched": [],
}
```

Beispiel für CloudWatch Logs Insights-Abfragen

Abfrage nach einer bestimmten Nachrichten-ID (zeigt den Nachrichtenfluss durch den Regelsatz):

```
fields @timestamp, @message, @logStream, @log
| filter message_id = 'message-id-123'
| sort @timestamp desc
| limit 10000
```

Abfrage nach fehlgeschlagenen WRITE_TO_S3-Aktionen:

```
fields @timestamp, @message, @logStream, @log
| filter action_metadata.action_name = 'WRITE_TO_S3'
    and action_metadata.action_status = 'FAILURE'
| sort @timestamp desc
| limit 10000
```

Abfrage nach Nachrichten, die nicht nach der zweiten Regel eines Regelsatzes verarbeitet wurden (die Nachricht erfüllte nicht die Bedingungen der Regel):

```
fields @timestamp, @message, @logStream, @log
| filter recipients_matched = '[]'
    and rule_index = 2
| sort @timestamp desc
| limit 10000
```

Amazon Simple Email Service Listen und Abonnements verwalten

Sie können Ihre eigenen Listen für Mailing und Abonnements sowie für die E-Mail-Unterdrückung in Amazon SES verwalten. Um Sie bei der Aufrechterhaltung Ihrer Senderreputation zu unterstützen, bietet SES Unterdrückung auf Konto- und Konfigurationssatzebene, die verhindert, dass Sie an ungültige Empfänger senden und Ihre Senderreputation schädigen. Als weitere Maßnahme gegen unzustellbare E-Mails und Beschwerden kann SES über die Abonnementverwaltung automatisch Abmeldelinks zu allen ausgehenden E-Mails hinzufügen.

Jeder dieser Listentypen wird in den Abschnitten, die in den Themen dieses Kapitels aufgeführt sind, ausführlich behandelt. Hier wird jedoch ein Überblick über die Unterdrückungslisten gegeben, um zu verstehen, wie sie sich unterscheiden, sowie eine wichtige Änderung bei der globalen Verwaltung von Unterdrückungslisten. Es wird empfohlen, diese Übersicht zu lesen, bevor Sie mit einer der in diesem Kapitel beschriebenen Listen arbeiten.

Überblick über Unterdrückungslisten und Mechanismen zur Überschreibung der Unterdrückung

Die Funktion zum Entfernen der globalen Unterdrückungsliste steht Kunden nicht mehr zur Verfügung, und Sie müssen nicht mehr mit ihr interagieren, um die Unterdrückung zu verwalten. Die globale Unterdrückungsliste funktioniert und wird im Hintergrund von SES verwaltet. Als Kunde stehen Ihnen jetzt eine Liste zur Unterdrückung von E-Mails auf Kontoebene und Einstellungen zur Verfügung, mit denen Sie die Unterdrückung von E-Mails für Ihr eigenes Konto individuell anpassen können.

Die verschiedenen Arten von Unterdrückungslisten, ihr Umfang und welche Vorteile sie bieten, werden im Folgenden erläutert.

- Globale Unterdrückungsliste — Eigentum von SES und verwaltet von SES, um den Ruf der Adressen im gemeinsam genutzten IP-Pool von SES zu schützen.
- Die Sperrliste auf Kontoebene — Eigentum des Kunden und wird von diesem verwaltet, um dessen Ruf zu schützen — hat Vorrang vor der globalen Sperrliste.
  - Unterdrückung auf Konfigurationssatzebene — Ein Überschreibungsmechanismus, der eine bedingte oder detaillierte Kontrolle der Unterdrückungsliste auf Kontoebene ermöglicht, indem die in einem Konfigurationssatz angegebenen Überschreibungen verwendet werden.

Die globale Unterdrückungsliste war die einzige Art der Unterdrückungsliste, bis die Unterdrückung auf Kontoebene und Konfigurationssatzebene in der neuen Amazon-SES-Konsole und API v2 eingeführt wurde. Die globale Unterdrückungsliste ist im Besitz von SES und wird von SES verwaltet, um die Reputation von SES zu schützen. Dies ist erforderlich, da sich alle SES-Kunden denselben IP-Adresspool teilen (sofern sie keine eigenen IP-Adressen haben IPs). Es ist daher wichtig, dass SES sicherstellt, dass Kunden keine Spam-Mails oder andere Dinge versenden, die sich negativ auf den Ruf dieser IP-Adressen im gemeinsam genutzten SES-IP-Pool auswirken könnten. Sie interagieren zwar nicht mehr direkt mit der globalen Unterdrückungsliste, sie arbeitet jedoch weiterhin im Hintergrund, und die allgemeinen Grundsätze der Funktionsweise der globalen Unterdrückungsliste können auch angewendet werden, um die allgemeinen Prinzipien der Funktionsweise der anderen Arten der Unterdrückung zu erklären. Siehe Globale Unterdrückungsliste in Amazon SES.

> **Note**
>
> Das Antragsformular zum Entfernen der globalen Unterdrückungsliste befindet sich nicht länger in der Amazon-SES-Konsole, da es durch die Unterdrückungsliste auf Kontoebene für alle in diesem Abschnitt erläuterten Vorteile ersetzt wurde.

Die Unterdrückungsliste auf Kontoebene wurde eingeführt, damit Kunden ihre eigene Unterdrückungsliste und ihren eigenen Ruf erstellen und kontrollieren können. Daher gilt die Unterdrückungsliste auf Kontoebene nur für Ihr Konto. Die Oberfläche der Unterdrückungsliste auf Kontoebene in der neuen Konsole bietet eine einfache Möglichkeit, Adressen in Ihrer Unterdrückungsliste auf Kontoebene zu verwalten, einschließlich Massenaktionen zum Hinzufügen oder Entfernen von Adressen. Wenn sich eine Adresse auf der globalen Unterdrückungsliste befindet, aber nicht auf Ihrer Unterdrückungsliste auf Kontoebene (was bedeutet, dass Sie an sie senden möchten) und Sie senden an sie, versucht Amazon SES dennoch eine Zustellung, aber wenn sie nicht zustellbar ist, wirkt sich die Unzustellbarkeit auf Ihren eigenen Ruf aus, aber niemand sonst erhält die Unzustellbarkeitsnachricht, weil er nicht an diese E-Mail-Adresse senden kann, wenn er nicht seine eigene Unterdrückungsliste auf Kontoebene verwendet; Daher überschreibt die Unterdrückungsliste auf Kontoebene die globale Unterdrückungsliste nur für Ihr Konto. Siehe Verwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole.

Die Unterdrückung auf Konfigurationssatzebene ist zwar keine Liste an sich, sondern ein Mechanismus, mit dem Sie mithilfe von Konfigurationssätzen, die speziell für verschiedene E-Mail-Versandszenarien erstellt wurden, Anpassungen und Überschreibungen für Ihre Unterdrückungsliste auf Kontoebene konfigurieren können. Angenommen, Ihre Unterdrückungsliste auf Kontoebene

ist so konfiguriert, dass sowohl Unzustellbarkeits- als auch Beschwerdeadressen hinzugefügt werden. Sie haben jedoch eine bestimmte E-Mail-Demografie in einem Konfigurationssatz definiert, für die nur Beschwerdeadressen hinzugefügt werden sollen. Dies würden Sie erreichen, indem Sie die Unterdrückungsüberschreibungen dieses Konfigurationssatzes aktivieren, sodass E-Mail-Adressen nur für Beschwerden (nicht für Unzustellbarkeit und Beschwerden, wie sie in Ihrer Unterdrückungsliste auf Kontoebene festgelegt sind) aus E-Mails, die mit diesem Konfigurationssatz gesendet wurden, Ihrer Unterdrückungsliste auf Kontoebene hinzugefügt werden. Bei der Unterdrückung auf Konfigurationssatzebene gibt es verschiedene Ebenen zum Überschreiben der Unterdrückung auf Kontoebene, einschließlich der Verwendung überhaupt keiner Unterdrückung. Siehe Verwenden der Unterdrückung auf Konfigurationssatzebene zum Überschreiben Ihrer Unterdrückungsliste auf Kontoebene.

Globale Unterdrückungsliste in Amazon SES

Amazon SES unterhält eine interne globale Unterdrückungsliste, das arbeitet und im Hintergrund von SES verwaltet wird. Wenn ein SES-Kunde eine E-Mail-Nachricht sendet, die zu einer permanenten Unzustellbarkeit führt, fügt SES die E-Mail-Adresse, die die Unzustellbarkeit erzeugt hat, zu einer globalen Unterdrückungsliste hinzu. Die globale Unterdrückungsliste ist global in dem Sinne, dass sie für alle SES-Kunden gilt. Anders gesagt, wenn ein anderer Kunde versucht, eine E-Mail an eine Adresse zu senden, die sich in der globalen Unterdrückungsliste befindet, akzeptiert SES die Nachricht, sendet sie aber nicht, da die E-Mail-Adresse unterdrückt wird.

Die Funktion zur Entfernung von E-Mail-Adressen auf der globalen Liste zur Entfernung von E-Mail-Adressen steht Kunden nicht mehr zur Verfügung und Sie können nicht mehr mit ihr interagieren, um die Unterdrückung zu verwalten. Um diese Funktion zu ersetzen, bietet Amazon SES Ihnen jetzt eine neue Möglichkeit, Ihre E-Mail-Unterdrückung zu verwalten, indem es eine Unterdrückungsliste auf Kontoebene und Überschreibungen für die Unterdrückung auf Konfigurationssatzebene zur Verfügung stellt, die Ihnen eine individuellere Kontrolle darüber bieten, wie Sie die E-Mail-Unterdrückung für Ihr eigenes Konto handhaben. Weitere Informationen erhalten Sie unter Verwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole und Verwenden der Unterdrückung auf Konfigurationssatzebene zum Überschreiben Ihrer Unterdrückungsliste auf Kontoebene.

> **Important**
>
> Das Antragsformular zum Entfernen der globalen Unterdrückungsliste für E-Mail-Adressen befindet sich nicht in der Amazon-SES-Konsole, da die Unterdrückungsliste auf Kontoebene ersetzt wurde. Weitere Informationen zur Verwendung der Unterdrückungsliste auf

Kontoebene siehe Verwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole.

Überlegungen zur globalen Unterdrückungsliste

Schlüsselfaktoren für die globale Unterdrückungsliste:

- Die globale Unterdrückungsliste funktioniert und wird im Hintergrund von SES verwaltet - Sie können nicht direkt damit interagieren; Sie können sie jedoch mithilfe Ihrer eigenen Unterdrückungsliste auf Kontoebene überschreiben.
- Die globale Unterdrückungsliste ist standardmäßig für alle SES-Konten aktiviert. Sie können es nicht deaktivieren.
- Da SES die globale Unterdrückungsliste auf alle Kunden anwendet, können Sie die globale Unterdrückungsliste nicht abfragen oder Adressen manuell hinzufügen.
- Wenn eine E-Mail-Adresse einen Hard Bounce erzeugt, fügt SES die Adresse der globalen Unterdrückungsliste für einen kurzen Zeitraum hinzu. Nach Ablauf dieses Zeitraums entfernt SES die Adresse aus der Liste. Wenn die Adresse einen weiteren Hard Bounce erzeugt, fügt SES diese für einen längeren Zeitraum wieder zur globalen Unterdrückungsliste hinzu und entfernt sie am Ende dieses Zeitraums. Die Zeit, die eine Adresse in der globalen Unterdrückungsliste verbleibt, erhöht sich jedes Mal, wenn die Adresse einen harten Bounce erzeugt. Eine E-Mail-Adresse kann bis zu 14 Tage lang in der globalen Unterdrückungsliste verbleiben.
- Wenn Sie versuchen, eine Nachricht an eine Adresse in der Unterdrückungsliste auf Kontoebene zu senden, akzeptiert SES die Nachricht, sendet sie aber nicht. SES generiert eine Bounce-Benachrichtigung mit einem `bounceType`-Wert von `Permanent`, und einem `bounceSubType`-Wert von `Suppressed`. Der Empfang dieser Art von Unzustellbarkeitsbenachrichtigung ist die einzige Möglichkeit, festzustellen, ob eine Adresse auf der globalen Unterdrückungsliste steht. Sie können die globale Unterdrückungsliste nicht abfragen.
- SES zählt die Nachrichten, die Sie an Adressen in der globalen Unterdrückungsliste senden, zur Unzustellbarkeitsrate für Ihr Konto und zu Ihrer täglichen Sendequote.
- Wie bei allen E-Mail-Adressen, die permanente Unzustellbarkeiten verursachen, sollten Sie Adressen entfernen, die Unzustellbarkeiten aufgrund der Unterdrückungsliste verursachen, es sei denn, Sie sind sicher, dass die Adresse gültig ist.
- Unzustellbarkeiten aufgrund der Unterdrückungsliste werden bei Ihrer Unzustellbarkeitsquote berücksichtigt. Wenn Ihre Unzustellbarkeitsrate zu hoch wird, wird Ihr Konto möglicherweise überprüft oder der E-Mail-Versand Ihres Kontos wird ausgesetzt.

> **Note**
>
> Es ist wichtig zu verstehen, wie die SES-Unterdrückungslisten miteinander verknüpft sind und welche Hierarchie sie haben. Weitere Informationen finden Sie unter Übersicht über Unterdrückungslisten und Mechanismen zur Aufhebung der Unterdrückung.

Verwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole

Die Amazon SES SES-Liste zur Unterdrückung auf Kontoebene wurde eingeführt, damit Kunden ihre eigene Sperrliste erstellen und kontrollieren und ihren Ruf verwalten können. Daher gilt Ihre Sperrliste auf Kontoebene nur für Ihr Konto. Die Oberfläche der Unterdrückungsliste auf Kontoebene in der SES-Konsole bietet eine einfache Möglichkeit, Adressen in Ihrer Unterdrückungsliste auf Kontoebene zu verwalten, einschließlich Massenaktionen zum Hinzufügen oder Entfernen von Adressen.

Ihre Unterdrückungsliste auf SES-Kontoebene gilt für Ihr AWS-Konto in der aktuellen AWS-Region. Mit SES API v2 oder der Konsole können Sie Adressen einzeln oder in Massen manuell zu Ihrer Unterdrückungsliste auf Kontoebene hinzufügen oder daraus entfernen.

> **Note**
>
> Um Adressen im Massenformat hinzuzufügen oder zu entfernen, müssen Sie über Produktionszugriff verfügen. Weitere Informationen zur Sandbox finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).

> **Important**
>
> Bei den Listen zur Unterdrückung von SES-Konten wird Groß- und Kleinschreibung beachtet. Wenn eine E-Mail-Adresse zur Sperrliste hinzugefügt wird, User@Example.com, wird sie genau so gespeichert, wie sie empfangen wurde, wobei die ursprüngliche Groß- und Kleinschreibung beibehalten wird. Während die E-Mail-Versandfunktion Adressen mit unterschiedlichen Groß- und Kleinschreibung als identisch behandelt, z. B. ist User@Example.com dasselbe wie user@example.com, erfordern API-Aufrufe für die Verwaltung der Unterdrückungsliste eine genaue Übereinstimmung zwischen Groß- und Kleinschreibung. Stellen Sie daher bei der Verwaltung von APIs Unterdrückungslisten sicher,

dass Sie die genaue Groß- und Kleinschreibung der E-Mail-Adresse verwenden, wie sie in der Unterdrückungsliste erscheint.

Überlegungen zur Unterdrückungsliste auf Kontoebene von Amazon SES

Sie sollten die folgenden Faktoren berücksichtigen, wenn Sie Ihre Unterdrückungsliste auf Kontoebene verwenden:

- Wenn Sie nach dem 25. November 2019 mit der Verwendung von Amazon SES begonnen haben, ist Ihr Konto so konfiguriert, dass die Unterdrückungsliste auf Kontoebene standardmäßig sowohl für Unzustellbarkeiten als auch für Beschwerden verwendet wird. Wenn mit der Verwendung von SES vor diesem Datum begonnen haben, müssen Sie diese Funktion mithilfe der Operation `PutAccountSuppressionAttributes` in der SES-API aktivieren.
- Wenn Sie versuchen, eine Nachricht an eine Adresse in der Unterdrückungsliste auf Kontoebene zu senden, deren Unterdrückungsgrund demjenigen entspricht, der für die Einstellungen für Unterdrückung auf Kontoebene ausgewählt wurde, akzeptiert SES die Nachricht, sendet sie aber nicht. Wenn sie allerdings nicht übereinstimmen, sendet SES die Nachricht. Dies wird in die folgenden Beispielen verdeutlicht:
  - Sie haben in Ihren Einstellungen für die Unterdrückung auf Kontoebene den Unterdrückungsgrund Nur Unzustellbare festgelegt. SES versucht nicht, an Adressen zuzustellen, die in Ihrer Unterdrückungsliste auf Kontoebene aufgeführt sind und für die der Unterdrückungsgrund Unzustellbarkeit angegeben ist. SES wird jedoch versuchen, Adressen in Ihrer Sperrliste auf Kontoebene mit dem Unterdrückungsgrund Beschwerde zuzustellen (da sie in diesem Fall nicht übereinstimmen).
  - Sie haben in Ihren Einstellungen für die Unterdrückung auf Kontoebene den Unterdrückungsgrund Unzustellbarkeit und Beschwerden festgelegt. SES versucht nicht, an Adressen zuzustellen, die in Ihrer Unterdrückungsliste auf Kontoebene aufgeführt sind und für die entweder der Unterdrückungsgrund Unzustellbarkeit oder Beschwerde angegeben ist.
- SES zählt die Nachrichten, die Sie an Adressen senden, die auf Ihrer Sperrliste auf Kontoebene stehen, nicht auf die Reputation. BounceRateoder Reputation. ComplaintRateMetriken im AWS/SES-Namespace für Ihr Konto. Solche Nachrichten werden unter den Metriken Bounce oder Complaint im /SES-Namespace gezählt. AWS
- Wenn sich eine Adresse auf der globalen Unterdrückungsliste, aber nicht auf Ihrer Unterdrückungsliste auf Kontoebene befindet (was bedeutet, dass Sie dorthin senden möchten) und Sie an diese Adresse senden, unternimmt SES immer noch einen Zustellversuch. Ist die

Nachricht allerdings unzustellbar, wird dies trotzdem auf die Unzustellbarkeitsrate Ihres Kontos und auf das tägliche Sendekontingent angerechnet.

- SES zählt die Nachrichten, die Sie an Adressen auf Ihrer Unterdrückungsliste auf Kontoebene senden, für Ihr täglich versendetes Kontingent.
- E-Mail-Adressen in Ihrer Unterdrückungsliste auf Kontoebene bleiben dort, bis Sie sie entfernen.
- Wenn die Fähigkeit Ihres Kontos zum Senden von E-Mail-Nachrichten unterbrochen wird, löscht SES automatisch nach 90 Tagen die Adressen in Ihrer Unterdrückungsliste auf Kontoebene. Wenn die Fähigkeit Ihres Kontos zum Senden von E-Mails vor Ablauf dieser 90-Tage wiederhergestellt wird, werden die Adressen in der Liste nicht gelöscht.
- Gmail stellt SES keine Beschwerdedaten zur Verfügung. Wenn ein Empfänger die Spam-Schaltfläche im Gmail-Webclient verwendet, um eine Nachricht, die er von Ihnen erhalten hat, als Spam zu melden, wird er nicht zu Ihrer Unterdrückungsliste auf Kontoebene hinzugefügt.
- Sie können Ihrer Unterdrückungsliste auf Kontoebene aktivieren, wenn sich Ihr Konto in der SES-Sandbox befindet. Sie können den CreateImportJobVorgang PutSuppressedDestinationoder jedoch erst verwenden, wenn Ihr Konto aus der Sandbox entfernt wurde. Weitere Informationen zur Sandbox finden Sie unter Produktionszugriff anfordern (Verlassen der Amazon SES SES-Sandbox).
- Nur permanent unzustellbare E-Mails werden Ihrer Unterdrückungsliste auf Kontoebene hinzugefügt. Informationen zu den Unterschieden zwischen temporär und permanent unzustellbaren E-Mails finden Sie unter the section called “Nachdem Amazon SES eine E-Mail gesendet hat”.
- Wenn Sie Ihre Unterdrückungsliste auf Kontoebene verwenden, fügt SES der globalen Unterdrückungsliste auch Adressen hinzu, die zu permanenten Unzustellbarkeiten führen.

> **Note**
>
> Bei den Verfahren in den folgenden Abschnitten wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Aktivieren der Unterdrückungsliste auf Kontoebene von Amazon SES

Sie können den PutAccountSuppressionAttributesVorgang in der Amazon SES API v2 verwenden, um Ihre Sperrliste auf Kontoebene zu aktivieren und einzurichten. Sie können diese Einstellung

schnell und einfach konfigurieren, indem Sie die AWS CLI verwenden. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im AWS Command Line Interface - Benutzerhandbuch.

Um Ihre Unterdrückungsliste auf Kontoebene zu konfigurieren, verwenden Sie die AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  Linux, macOS, or Unix

  ```
  aws sesv2 put-account-suppression-attributes \
  --suppressed-reasons BOUNCE COMPLAINT
  ```

  Windows

  ```
  aws sesv2 put-account-suppression-attributes `
  --suppressed-reasons BOUNCE COMPLAINT
  ```

  Um Ihre Unterdrückungsliste auf Kontoebene zu aktivieren, müssen Sie für den Parameter `suppressed-reasons` mindestens einen Grund angeben. Sie können entweder `BOUNCE` oder `COMPLAINT` angeben oder Sie können beides angeben, wie im vorherigen Beispiel gezeigt.

So konfigurieren Sie Ihre Unterdrückungsliste auf Kontoebene mit der SES-Konsole:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. Wählen Sie in Account-level settings (Einstellungen auf Kontoebene), Edit (Bearbeiten) aus.
4. Aktivieren Sie in der Suppression list (Unterdrückungsliste) das Kontrollkästchen Enabled (Aktiviert).
5. Wählen Sie unter Suppression reasons (Unterdrückungsgründe) einen der Gründe aus, aus denen Empfänger-E-Mail-Adressen automatisch zu Ihrer Unterdrückungsliste auf Kontoebene hinzugefügt werden sollen.
6. Wählen Sie Änderungen speichern aus.

Aktivieren der Unterdrückungsliste auf Kontoebene von Amazon SES für einen Konfigurationssatz

Sie können Ihre Unterdrückung auf Kontoebene von Amazon SES auch so konfigurieren, dass sie nur für bestimmte Konfigurationssätze gilt. Wenn Sie dies tun, werden Adressen der Unterdrückungsliste nur hinzugefügt, wenn Sie den Konfigurationssatz beim Senden der E-Mail-Nachricht angegeben haben, die das Unzustellbarkeits- oder Beschwerdeereignis verursacht hat.

Um Ihre Unterdrückungsliste auf Kontoebene für einen Konfigurationssatz zu konfigurieren, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  Linux, macOS, or Unix

  ```
  aws sesv2 put-configuration-set-suppression-options \
  --configuration-set-name configSet \
  --suppressed-reasons BOUNCE COMPLAINT
  ```

  Windows

  ```
  aws sesv2 put-configuration-set-suppression-options `
  --configuration-set-name configSet `
  --suppressed-reasons BOUNCE COMPLAINT
  ```

  Ersetzen Sie es im vorherigen Beispiel *configSet* durch den Namen des Konfigurationssatzes, der Ihre Unterdrückungsliste auf Kontoebene verwenden soll.

So konfigurieren Sie Ihre Unterdrückungsliste auf Kontoebene mit der SES-Konsole:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Configuration sets (Konfigurationssätze) aus.
3. Wählen Sie unter Configuration sets (Konfigurationssätze) den Namen des Konfigurationssatzes aus, den Sie mit benutzerdefinierter Unterdrückung konfigurieren möchten.

4. Wählen Sie im Bereich Suppression list options (Optionen der Unterdrückungsliste) die Option Edit (Bearbeiten) aus.
5. Der Abschnitt Suppression list options (Unterdrückungslistenoptionen) enthält eine Entscheidungsgruppe zum Definieren einer benutzerdefinierten Unterdrückung, beginnend mit der Option, diese Konfiguration zu verwenden, um Ihre Unterdrückung auf Kontoebene zu überschreiben. Die Logik-Map für die Unterdrückung auf Satzebene hilft Ihnen, die Auswirkungen der Überschreibungskombinationen zu verstehen. Diese mehrschichtige Auswahl an Überschreibungen kann kombiniert werden, um drei verschiedene Unterdrückungsebenen zu implementieren:

   a. Verwenden Sie Unterdrückung auf Kontoebene: Überschreiben Sie Ihre Unterdrückung auf Kontoebene nicht und implementieren Sie keine Unterdrückung auf Konfigurationssatzebene. Grundsätzlich verwendet jede E-Mail, die mit diesem Konfigurationssatz gesendet wird, nur Ihre Unterdrückung auf Kontoebene. So gehen Sie vor:

      - Deaktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

   b. Verwenden Sie keine Unterdrückung: Überschreiben Sie die Unterdrückung auf Kontoebene, ohne die Unterdrückung auf Konfigurationssatzebene zu aktivieren. Dies bedeutet, dass alle mit diesem Konfigurationssatz gesendeten E-Mails keine Unterdrückung auf Kontoebene verwenden – mit anderen Worten, jede Unterdrückung wird aufgehoben. So gehen Sie vor:

      i. Aktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

      ii. Deaktivieren Sie in der Suppression list (Unterdrückungsliste) das Kontrollkästchen Enabled (Aktiviert).

   c. Verwenden Sie die Unterdrückung auf Satzebene auf Konfiguration: Überschreiben Sie Ihre Unterdrückung auf Kontoebene mit benutzerdefinierten Einstellungen für Unterdrückungslisten, die in diesem Konfigurationssatz definiert sind. Dies bedeutet, dass jede E-Mail, die mit diesem Konfigurationssatz gesendet wird, nur ihre eigenen Unterdrückungseinstellungen verwendet und alle Unterdrückungseinstellungen auf Kontoebene ignoriert. So gehen Sie vor:

i. Aktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

ii. Wählen Sie in der Suppression list (Unterdrückungsliste) Enabled (Aktiviert) aus.

iii. Wählen Sie in Specify the reason(s)... (Geben Sie den Grund(e) an ...) einen der Unterdrückungsgründe für diese zu verwendende Konfiguration aus.

6. Wählen Sie Änderungen speichern aus.

Hinzufügen einzelner E-Mail-Adressen zur Unterdrückungsliste auf Kontoebene von Amazon SES

Sie können einzelne Adressen zu Ihrer Amazon SES SES-Unterdrückungsliste auf Kontoebene hinzufügen, indem Sie den PutSuppressedDestinationVorgang in der SES-API v2 verwenden. Es gibt keine Begrenzung für die Anzahl der Adressen, die Sie Ihrer Unterdrückungsliste auf Kontoebene hinzufügen können.

Um einzelne Adressen zu Ihrer Sperrliste auf Kontoebene hinzuzufügen, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  Linux, macOS, or Unix

  ```
  aws sesv2 put-suppressed-destination \
  --email-address recipient@example.com \
  --reason BOUNCE
  ```

  Windows

  ```
  aws sesv2 put-suppressed-destination `
  --email-address recipient@example.com `
  --reason BOUNCE
  ```

  *recipient@example.com*Ersetzen Sie im vorherigen Beispiel durch die E-Mail-Adresse, die Sie zu Ihrer Unterdrückungsliste auf Kontoebene hinzufügen möchten, und *BOUNCE* durch den Grund, warum Sie die Adresse zur Unterdrückungsliste hinzufügen möchten (zulässige Werte sind und). `BOUNCE` `COMPLAINT`

So fügen Sie mit der SES-Konsole individuelle Adressen zu Ihrer Unterdrückungsliste auf Kontoebene hinzu:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. Wählen Sie im Bereich Suppression list (Unterdrückungsliste) die Option Add email (E-Mail-Adresse hinzufügen) aus.
4. Geben Sie unter Email address (E-Mail-Adresse) eine E-Mail-Adresse ein, wählen Sie unter Suppression reason (Unterdrückungsgrund) einen Grund aus. Wenn Sie weitere Adressen eingeben müssen, wählen Sie Enter another address (Weitere Adresse eingeben) und wiederholen Sie den Vorgang für jede weitere.
5. Wenn Sie mit der Eingabe von Adressen fertig sind, überprüfen Sie, dass Ihre Einträge korrekt sind. Wenn Sie entscheiden, dass einer Ihrer Einträge nicht Teil dieser Einreichung sein sollte, wählen Sie die Schaltfläche Remove (Entfernen) aus.
6. Klicken Sie auf Save changes (Änderungen speichern), um die eingegebenen E-Mail-Adressen zur Unterdrückungsliste auf Kontoebene hinzuzufügen.

Hinzufügen von E-Mail-Adressen in Ihrer Unterdrückungsliste auf Kontoebene von Amazon SES

Sie können mehrere Adressen gleichzeitig hinzufügen, indem Sie zuerst Ihre Kontaktliste in ein Amazon S3 S3-Objekt hochladen und anschließend den CreateImportJobVorgang in der Amazon SES API v2 verwenden.

> **Note**
>
> - Es gibt keine Begrenzung für die Anzahl der Adressen, die Sie Ihrer Unterdrückungsliste auf Kontoebene hinzufügen können, aber es gibt ein Bulk-Add-Limit von 100.000 Adressen in einem Amazon S3 Objekt pro API-Aufruf.
> - Sie können nicht mehr als 20 Importaufträge gleichzeitig ausführen.
> - Wenn es sich bei Ihrer Datenquelle um einen S3-Bucket handelt, muss dieser in derselben Region vorhanden sein, in die Sie importieren.

Führen Sie die folgenden Schritte aus, um der Unterdrückungsliste auf Kontoebene mehrere E-Mail-Adressen hinzuzufügen.

- Laden Sie Ihre Adressliste in ein Amazon S3 Objekt im CSV- oder JSON-Format hoch.

  CSV-Format Beispiel zum Hinzufügen von Adressen:

  recipient1@example.com,*BOUNCE*

  recipient2@example.com,*COMPLAINT*

  Nur durch Zeilenzeichen getrennte JSON-Dateien werden unterstützt. In diesem Format ist jede Zeile ein vollständiges JSON-Objekt, das eine individuelle Adressdefinition enthält.

  Beispiel für das JSON-Format zum Hinzufügen von Adressen:

  {"emailAddress":"*recipient1@example.com*","reason":"*BOUNCE*"}

  {"emailAddress":"*recipient2@example.com*","reason":"*COMPLAINT*"}

  Ersetzen Sie in den vorherigen Beispielen *recipient1@example.com* und *recipient2@example.com* durch die E-Mail-Adressen, die Sie zu Ihrer Unterdrückungsliste auf Kontoebene hinzufügen möchten. Die zulässigen Gründe, aus denen Sie die Adressen zur Unterdrückungsliste hinzufügen, sind*BOUNCE* und *COMPLAINT*.
- Erteilen Sie SES die Berechtigung zur Verwendung Ihres AWS KMS -Schlüssels.

  Wenn das Amazon S3 S3-Objekt mit einem AWS KMS Schlüssel verschlüsselt ist, müssen Sie Amazon SES die Erlaubnis zur Verwendung des AWS KMS Schlüssels erteilen. SES kann nur die Berechtigung von einem vom Kunden verwalteten Schlüssel erhalten, nicht von einem standardmäßigen KMS-Schlüssel. Bei Verwendung eines benutzerdefinierten Hauptschlüssels müssen Sie SES die entsprechende Berechtigung erteilen, indem Sie der Richtlinie des Schlüssels eine Anweisung hinzufügen.

  Fügen Sie die folgende Richtlinienanweisung in die Schlüsselrichtlinie ein, um SES zu erlauben, Ihren vom Kunden verwalteten Schlüssel zu verwenden.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
```

```
    },
    "Action": [
        "kms:Decrypt",
    ],
    "Resource": "*"
}
```

- Verwenden Sie den CreateImportJobVorgang in der SES-API v2.

> **Note**
>
> Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Geben Sie in der Befehlszeile den folgenden Befehl ein: *s3bucket*Ersetzen Sie durch den Namen eines Amazon S3 S3-Buckets und *s3object* durch den Namen eines Amazon S3 S3-Objekts.

```
aws sesv2 create-import-job --import-destination
 SuppressionListDestination={SuppressionListImportAction=PUT} --import-data-source
 S3Url=s3://s3bucket/s3object,DataFormat=CSV
```

So fügen Sie mit der SES-Konsole E-Mail-Adressen in großen Mengen zu Ihrer Unterdrückungsliste auf Kontoebene hinzu:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. Erweitern Sie in der Tabelle der Suppression list (Unterdrückungsliste) die Schaltfläche Bulk actions (Massenaktionen) und wählen Sie Add email addresses in bulk (E-Mail-Adressen in Massen hinzufügen) aus.
4. Wählen Sie in den Bulk action specifications (Massenaktionsspezifikationen) entweder (a)Choose file from S3 bucket (Datei aus S3-Bucket auswählen) oder (b)Import from file (Aus Datei importieren) – Verfahren werden für jede Importmethode angegeben:

a. Choose file from S3 bucket (Wählen Sie eine Datei aus dem S3 Bucket) – wenn Ihre Quelldatei bereits in einem Amazon-S3-Bucket gespeichert ist:

   i. Wenn Sie den URI des Amazon-S3-Buckets kennen, den Sie verwenden möchten, geben Sie ihn in das Feld Amazon-S3-URI ein; andernfalls wählen Sie Browse S3 (S3 durchsuchen) aus:

      A. Wählen Sie unter Buckets den Namen des S3 Buckets aus.

      B. Wählen Sie unter Objects (Objekte) den Namen der Datei aus und wählen Sie dann Choose (Auswählen) aus – Sie kehren zu den Bulk action specifications (Massenaktionsspezifikationen) zurück.

      C. (Optional) Wenn Sie zur Amazon-S3-Konsole weitergeleitet werden möchten, um Details zu Ihrem S3-Objekt anzuzeigen, wählen Sie View (Anzeigen) aus.

   ii. Wählen Sie unter File format (Dateiformat) das Format der Datei aus, die Sie zum Importieren aus Ihrem Amazon-S3-Bucket ausgewählt haben.

   iii. Wählen Sie Add email addresses (E-Mail-Adressen hinzufügen) aus, um den Import von Adressen aus Ihrer Datei zu starten – eine Tabelle unter Bulk actions (Massenaktionen) wird angezeigt.

b. Import from file (Aus Datei importieren) – wenn Sie eine lokale Quelldatei zum Hochladen in einen neuen oder vorhandenen Amazon-S3-Bucket haben:

   i. Wählen Sie unter Import source file (Importieren einer Quelldatei) Choose file (Datei auswählen).

   ii. Wählen Sie die JSON- oder CSV-Datei im Dateibrowser aus und wählen Sie Open (Öffnen) – Sie sehen den Namen, die Größe und das Datum Ihrer Datei unter Choose file (Datei auswählen).

   iii. Erweitern Sie Amazon-S3-Bucket und wählen Sie den S3 Bucket aus.

      - Um Ihre Datei in einen neuen Bucket hochzuladen, wählen Sie Create S3 bucket (S3 Bucket erstellen), geben Sie einen Namen in das Feld Bucket name (Bucket-Name) ein und wählen Sie Create bucket (Bucket erstellen) aus.

   iv. Wählen Sie Add email addresses (E-Mail-Adressen hinzufügen) aus, um den Import von Adressen aus Ihrer Datei zu starten – eine Tabelle unter Bulk actions (Massenaktionen) wird angezeigt.

5. Unabhängig von der von Ihnen verwendeten Importmethode wird Ihre Auftrags-ID in Bulk actions (Massenaktionen) zusammen mit Importtyp, Status und Datum aufgeführt. Um Auftragsdetails anzuzeigen, wählen Sie die Auftrags-ID aus.
6. Wählen Sie Suppression list (Unterdrückungsliste) aus und alle erfolgreich importierten E-Mail-Adressen werden mit Grund und Datum für die Unterdrückung angezeigt – die folgenden Optionen sind verfügbar:

    a. Wählen Sie eine E-Mail-Adresse aus oder aktivieren Sie das entsprechende Kontrollkästchen und wählen Sie View report (Bericht anzeigen) um ihre Details anzuzeigen. (Wenn es sich um eine Adresse handelt, die aufgrund einer Unzustellbarkeit oder einer Beschwerde automatisch zu Ihrer Unterdrückungsliste hinzugefügt wurde, werden Informationen über das Feedback-Ereignis angezeigt, das das Hinzufügen verursacht hat, einschließlich Details über die E-Mail-Nachricht, die das auslösende Ereignis ausgelöst hat.)

    b. Aktivieren Sie das entsprechende Kontrollkästchen für eine oder mehrere E-Mail-Adressen, die Sie aus Ihrer Kontounterdrückungsliste entfernen möchten und wählen Sie Remove (Entfernen) aus.

Anzeigen einer Liste der Adressen, die sich in Ihrer Unterdrückungsliste auf Kontoebene von Amazon SES befinden

Mithilfe des ListSuppressedDestinationsVorgangs in der SES-API v2 können Sie sich eine Liste aller E-Mail-Adressen anzeigen lassen, die auf Ihrer Sperrliste auf Kontoebene für Ihr Konto stehen.

Anzeigen einer Liste aller E-Mail-Adressen, die sich in Ihrer Unterdrückungsliste auf Kontoebene befinden

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 list-suppressed-destinations
```

Mit dem obigen Befehl werden alle E-Mail-Adressen zurückgegeben, die sich in Ihrem Konto in Ihrer Unterdrückungsliste auf Kontoebene befinden. Die Ausgabe sieht in etwa folgendermaßen aus:

```
{
    "SuppressedDestinationSummaries": [
        {
            "EmailAddress": "recipient2@example.com",
```

```
            "Reason": "COMPLAINT",
            "LastUpdateTime": "2020-04-10T21:03:05Z"
        },
        {
            "EmailAddress": "recipient0@example.com",
            "Reason": "COMPLAINT",
            "LastUpdateTime": "2020-04-10T21:04:26Z"
        },
        {
            "EmailAddress": "recipient1@example.com",
            "Reason": "BOUNCE",
            "LastUpdateTime": "2020-04-10T22:07:59Z"
        }
    ]
}
```

- Hinweis — Wenn Ihre Ausgabe ein Feld "NextToken" mit einem Zeichenfolgenwert enthält, bedeutet dies, dass die Unterdrückungsliste für Ihr Konto weitere E-Mail-Adressen enthält. Um zusätzliche unterdrückte Adressen anzuzeigen, stellen Sie eine weitere Anfrage an `ListSuppressedDestinations`, und übergeben Sie den zurückgegebenen String-Wert im `--next-token`-Parameter wie folgt:

  ```
  aws sesv2 list-suppressed-destinations --next-token string
  ```

  Ersetzen Sie im vorherigen Befehl durch *`string`* den zurückgegebenen NextToken Wert.

  Weitere Informationen finden Sie unter So führen Sie über 1000 E-Mail-Adressen aus der Unterdrückungsliste auf Kontoebene auf.

Sie können die `StartDate`-Option verwenden, um nur E-Mail-Adressen anzuzeigen, die der Liste nach einem bestimmten Datum hinzugefügt wurden.

Anzeigen einer Liste der Adressen, die Ihrer Unterdrückungsliste auf Kontoebene nach einem bestimmten Datum hinzugefügt wurden

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws sesv2 list-suppressed-destinations --start-date 1604394130
  ```

  Ersetzen Sie im vorherigen Befehl *`1604394130`* durch den Unix-Zeitstempel des Startdatums.

Sie können die `EndDate` Option auch verwenden, um nur E-Mail-Adressen anzuzeigen, die der Liste vor einem bestimmten Datum hinzugefügt wurden.

Anzeigen einer Liste der Adressen, die Ihrer Unterdrückungsliste auf Kontoebene vor einem bestimmten Datum hinzugefügt wurden

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws sesv2 list-suppressed-destinations --end-date 1611126000
  ```

  Ersetzen Sie im vorherigen Befehl *1611126000* durch den Unix-Zeitstempel des Enddatums.

In der Linux-, macOS- oder Unix-Befehlszeile können Sie auch das integrierte `grep`-Dienstprogramm verwenden, um nach bestimmten Adressen oder Domänen zu suchen.

Suchen einer bestimmten Adresse in Ihrer Unterdrückungsliste auf Kontoebene

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws sesv2 list-suppressed-destinations | grep -A2 'example.com'
  ```

  Ersetzen Sie im vorherigen Befehl *example.com* durch die Textzeichenfolge (z. B. die Adresse oder Domäne), nach der Sie suchen möchten.

Zum Anzeigen einer Liste aller E-Mail-Adressen, die sich in Ihrer Unterdrückungsliste auf der Kontoebene befinden, verwenden Sie die SES-Konsole:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. In der Suppression list (Unterdrückungsliste) werden alle E-Mail-Adressen in Ihrer Unterdrückungsliste auf Kontoebene angezeigt, wobei der Grund und das Datum der Unterdrückung hinzugefügt werden – die folgenden Optionen sind verfügbar:

   a. Wählen Sie eine E-Mail-Adresse aus oder aktivieren Sie das entsprechende Kontrollkästchen und wählen Sie View report (Bericht anzeigen) um ihre Details anzuzeigen.

(Wenn es sich um eine Adresse handelt, die aufgrund einer Unzustellbarkeit oder einer Beschwerde automatisch zu Ihrer Unterdrückungsliste hinzugefügt wurde, werden Informationen über das Feedback-Ereignis angezeigt, das das Hinzufügen verursacht hat, einschließlich Details über die E-Mail-Nachricht, die das auslösende Ereignis ausgelöst hat.)

b. Sie können die Unterdrückungslistentabelle anpassen, indem Sie das Zahnradsymbol auswählen – ein Modal wird angezeigt, in dem Sie die Seitengröße, den Zeilenumbruch und die anzuzeigenden Spalten anpassen können – nachdem Sie Ihre Auswahl getroffen haben, wählen Sie Confirm (Bestätigen). Die Tabelle der Unterdrückungsliste spiegelt Ihre Anzeigeoptionen wider.

Löschen einzelner E-Mail-Adressen aus Ihrer Unterdrückungsliste auf Kontoebene von Amazon SES

Wenn eine Adresse auf der Sperrliste für Ihr Konto steht, Sie aber wissen, dass die Adresse nicht auf der Liste stehen sollte, können Sie sie mithilfe der DeleteSuppressedDestinationOperation in der SES-API v2 entfernen.

Um einzelne Adressen aus Ihrer Sperrliste auf Kontoebene zu entfernen, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  Linux, macOS, or Unix

  ```
  aws sesv2 delete-suppressed-destination \
  --email-address recipient@example.com
  ```

  Windows

  ```
  aws sesv2 delete-suppressed-destination `
  --email-address recipient@example.com
  ```

  Ersetzen Sie es im vorherigen Beispiel *recipient@example.com* durch die E-Mail-Adresse, die Sie aus Ihrer Sperrliste auf Kontoebene entfernen möchten.

So entfernen Sie mit der SES-Konsole einzelne Adressen aus Ihrer Unterdrückungsliste auf Kontoebene:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. Entfernen Sie einzelne E-Mail-Adressen entweder über (a) eine Tabellenauswahl oder (b) einen getippten Eintrag:

    a. Auswahl aus Tabelle: Aktivieren Sie in der Tabelle Suppression list (Unterdrückungsliste) das entsprechende Kontrollkästchen einer oder mehrerer E-Mail-Adressen und wählen Sie Remove (Entfernen) aus.

    b. Eingabe in Feld:

        i. Wählen Sie in der Tabelle Suppression list (Unterdrückungsliste) die Option Remove email address (E-Mail-Adresse entfernen) aus.

        ii. Geben Sie im Feld Email address (E-Mail-Adresse) eine E-Mail-Adresse ein. Wenn Sie weitere Adressen eingeben müssen, wählen Sie Enter another address (Weitere Adresse eingeben) aus und wiederholen Sie den Vorgang für jede weitere.

        iii. Wenn Sie mit der Eingabe von Adressen fertig sind, überprüfen Sie, dass Ihre Einträge korrekt sind. Wenn Sie entscheiden, dass einer Ihrer Einträge nicht Teil dieser Einreichung sein sollte, wählen Sie die Schaltfläche Remove (Entfernen) aus.

        iv. Klicken Sie auf Save changes (Änderungen speichern), um die eingegebenen E-Mail-Adressen aus der Unterdrückungsliste auf Kontoebene zu entfernen.

Entfernen von E-Mail-Adressen aus Ihrer Unterdrückungsliste auf Kontoebene von Amazon SES

Sie können mehrere Adressen gleichzeitig entfernen, indem Sie zuerst Ihre Kontaktliste in ein Amazon S3 S3-Objekt hochladen und anschließend den CreateImportJobVorgang in der SES-API v2 verwenden.

> **Note**
>
> - Für die Anzahl der Adressen, die Sie aus der Unterdrückungsliste auf Kontoebene entfernen können, gibt es jedoch ein Massenlöschlimit von 10.000 Adressen in einem Amazon S3 Objekt pro API-Aufruf.
> - Wenn es sich bei Ihrer Datenquelle um einen S3-Bucket handelt, muss dieser in derselben Region vorhanden sein, in die Sie importieren.

Führen Sie die folgenden Schritte aus, um Massen-E-Mail-Adressen aus der Unterdrückungsliste auf Kontoebene zu entfernen.

- Laden Sie Ihre Adressliste in ein Amazon S3 Objekt im CSV- oder JSON-Format hoch.

  CSV-Format Beispiel zum Entfernen von Adressen:

  recipient3@example.com

  Nur durch Zeilenzeichen getrennte JSON-Dateien werden unterstützt. In diesem Format ist jede Zeile ein vollständiges JSON-Objekt, das eine individuelle Adressdefinition enthält.

  Beispiel für das JSON-Format zum Hinzufügen von Adressen:

  `{"emailAddress":"`*recipient3@example.com*`"}`

  Ersetzen Sie diese in den vorherigen Beispielen *recipient3@example.com* durch die E-Mail-Adressen, die Sie aus Ihrer Sperrliste auf Kontoebene entfernen möchten.
- Erteilen Sie SES Berechtigung, das Amazon S3 Objekt zu lesen.

  Bei Anwendung auf einen Amazon-S3-Bucket erteilt die folgenden Richtlinie SES die Berechtigung zum Schreiben von Daten in diesen Bucket. Weitere Informationen zu Bucket-Richtlinien für Amazon S3 finden Sie unter Verwenden von Bucket-Richtlinien und Benutzerrichtlinien im Entwicklerhandbuch zu Amazon Simple Storage Service.
- Erteilen Sie SES die Erlaubnis, Ihren AWS KMS Schlüssel zu verwenden.

  Wenn das Amazon S3 S3-Objekt mit einem AWS KMS Schlüssel verschlüsselt ist, müssen Sie Amazon SES die Erlaubnis zur Verwendung des AWS KMS Schlüssels erteilen. SES kann nur die Berechtigung von einem vom Kunden verwalteten Schlüssel erhalten, nicht von einem standardmäßigen KMS-Schlüssel. Bei Verwendung eines benutzerdefinierten Hauptschlüssels

müssen Sie SES die entsprechende Berechtigung erteilen, indem Sie der Richtlinie des Schlüssels eine Anweisung hinzufügen.

Fügen Sie die folgende Richtlinienanweisung in die Schlüsselrichtlinie ein, um SES zu erlauben, Ihren vom Kunden verwalteten Schlüssel zu verwenden.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Verwenden Sie den CreateImportJobVorgang in der SES-API v2.

> **Note**
>
> Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Geben Sie in der Befehlszeile den folgenden Befehl ein: *s3bucket*Ersetzen Sie durch den Namen des Amazon S3 S3-Buckets und *s3object* durch den Namen des Amazon S3 S3-Objekts.

```
aws sesv2 create-import-job --import-destination
 SuppressionListDestination={SuppressionListImportAction=DELETE} --import-data-source
 S3Url="s3://s3bucket/s3object",DataFormat=CSV
```

So entfernen Sie E-Mail-Adressen mit der SES-Konsole in großen Mengen aus Ihrer Unterdrückungsliste auf Kontoebene:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.

2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. Erweitern Sie in der Tabelle der Suppression list (Unterdrückungsliste) die Schaltfläche Bulk actions (Massenaktionen) und wählen Sie Remove email addresses in bulk (E-Mail-Adressen in Massen entfernen) aus.
4. Wählen Sie in den Bulk action specifications (Massenaktionsspezifikationen) entweder (a) Choose file from S3 bucket (Datei aus S3-Bucket auswählen) oder (b) Import from file (Aus Datei importieren) – Verfahren werden für jede Importmethode angegeben:

    a. Choose file from S3 bucket (Wählen Sie eine Datei aus dem S3 Bucket) – wenn Ihre Quelldatei bereits in einem Amazon-S3-Bucket gespeichert ist:

        i. Wenn Sie den URI des Amazon-S3-Buckets kennen, den Sie verwenden möchten, geben Sie ihn in das Feld Amazon-S3-URI ein; andernfalls wählen Sie Browse S3 (S3 durchsuchen) aus:

            A. Wählen Sie unter Buckets den Namen des S3 Buckets aus.

            B. Wählen Sie unter Objects (Objekte) den Namen der Datei aus und wählen Sie dann Choose (Auswählen) aus – Sie kehren zu den Bulk action specifications (Massenaktionsspezifikationen) zurück.

            C. (Optional) Wenn Sie zur Amazon-S3-Konsole weitergeleitet werden möchten, um Details zu Ihrem S3-Objekt anzuzeigen, wählen Sie View (Anzeigen) aus.

        ii. Wählen Sie unter File format (Dateiformat) das Format der Datei aus, die Sie zum Importieren aus Ihrem Amazon-S3-Bucket ausgewählt haben.

        iii. Wählen Sie Remove email addresses (Entfernen von E-Mail-Adressen) aus, um den Import von Adressen aus Ihrer Datei zu starten – eine Tabelle unter Bulk actions (Massenaktionen) wird angezeigt.

    b. Import from file (Aus Datei importieren) – wenn Sie eine lokale Quelldatei zum Hochladen in einen neuen oder vorhandenen Amazon-S3-Bucket haben:

        i. Wählen Sie unter Import source file (Importieren einer Quelldatei) Choose file (Datei auswählen).

        ii. Wählen Sie die JSON- oder CSV-Datei im Dateibrowser aus und wählen Sie Open (Öffnen) – Sie sehen den Namen, die Größe und das Datum Ihrer Datei unter Choose file (Datei auswählen).

        iii. Erweitern Sie Amazon-S3-Bucket und wählen Sie den S3 Bucket aus.

- Um Ihre Datei in einen neuen Bucket hochzuladen, wählen Sie Create S3 bucket (S3 Bucket erstellen), geben Sie einen Namen in das Feld Bucket name (Bucket-Name) ein und wählen Sie Create bucket (Bucket erstellen) aus.

iv. Wählen Sie Remove email addresses (Entfernen von E-Mail-Adressen) aus, um den Import von Adressen aus Ihrer Datei zu starten – eine Tabelle unter Bulk actions (Massenaktionen) wird angezeigt.

5. Unabhängig von der von Ihnen verwendeten Importmethode wird Ihre Auftrags-ID in Bulk actions (Massenaktionen) zusammen mit Importtyp, Status und Datum aufgeführt. Um Auftragsdetails anzuzeigen, wählen Sie die Auftrags-ID aus.
6. Wählen Sie die Registerkarte Suppression list (Unterdrückungsliste) und alle erfolgreich importierten E-Mail-Adressen, die aus Ihrer Unterdrückungsliste entfernt wurden, werden nicht mehr angezeigt.

Anzeigen einer Liste von Importaufträgen für das Konto

Mithilfe des ListImportJobsVorgangs in der Amazon SES API v2 können Sie eine Liste aller E-Mail-Adressen anzeigen, die auf Ihrer Sperrliste auf Kontoebene für Ihr Konto stehen.

So zeigen Sie eine Liste aller Importaufträge für das Konto an

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 list-import-jobs
```

Der obige Befehl gibt alle Importaufträge für das Konto zurück. Die Ausgabe sieht in etwa folgendermaßen aus:

```
{
    "ImportJobs": [
        {
            "CreatedTimestamp": 2020-07-31T06:06:55Z",
            "ImportDestination": {
                "SuppressionListDestination": {
                    "SuppressionListImportAction": "PUT"
                }
            },
            "JobStatus": "COMPLETED",
```

```
            "JobId": "755380d7-fbdb-4ed2-a9a3-06866220f5b5"
        },
        {
            "CreatedTimestamp": "2020-07-30T18:45:32Z",
            "ImportDestination": {
                "SuppressionListDestination": {
                    "SuppressionListImportAction": "DELETE"
                }
            },
            "JobStatus": "COMPLETED",
            "JobId": "076683bd-a7ee-4a40-9754-4ad1161ba8b6"
        },
        {
            "CreatedTimestamp": "2020-08-05T16:45:18Z",
            "ImportDestination": {
                "SuppressionListDestination": {
                    "SuppressionListImportAction": "PUT"
                }
            },
            "JobStatus": "COMPLETED",
            "JobId": "6e261869-bd30-4b33-b1f2-9e035a83a395"
        }
    ]
}
```

So zeigen Sie eine Liste aller Importaufträge für das Konto mit der SES-Konsole an:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. Wählen Sie in der Suppression list (Unterdrückungsliste) die Option Bulk actions (Massenaktionen) aus.
4. Alle Importaufträge werden im Feld Bulk actions (Massenaktionen) als Tabelle zusammen mit Importtyp, Status und Datum aufgelistet.
5. Um Auftragsdetails anzuzeigen, wählen Sie die Auftrags-ID aus und die folgenden Bereiche werden angezeigt:

a. Massenaktionsstatus: zeigt den Gesamtstatus der Aufträge, die Uhrzeit und das Datum, an dem sie abgeschlossen wurden an, wie viele Datensätze importiert wurden und die Anzahl aller Datensätze, die nicht erfolgreich importiert wurden.

b. Details zur Massenaktion: zeigt die Auftrags-ID an, unabhängig davon, ob sie zum Hinzufügen oder Entfernen von Adressen verwendet wurde, ob das Dateiformat JSON oder CSV war, den URI des Amazon-S3-Buckets, in dem die Massendatei gespeichert wurde, sowie Uhrzeit und Datum, an dem die Massenaktion erstellt wurde.

Abrufen von Informationen über einen Importauftrag für das Konto

Sie können Informationen zu einem Importauftrag für das Konto abrufen, indem Sie den GetImportJobVorgang in der Amazon SES API v2 verwenden.

So rufen Sie Informationen über einen Importauftrag für das Konto ab

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 get-import-job --job-id JobId
```

Mit dem vorherigen Befehl werden Informationen über einen Importauftrag für das Konto zurückgegeben. Die Ausgabe sieht in etwa folgendermaßen aus:

```
{
    "ImportDataSource": {
        "S3Url": "s3://bucket/object",
        "DataFormat": "CSV"
    },
    "ProcessedRecordsCount": 2,
    "FailureInfo": {
        "FailedRecordsS3Url": "s3presignedurl"
    },
    "JobStatus": "COMPLETED",
    "JobId": "jobid",
    "CreatedTimestamp": "2020-08-12T17:05:15Z",
    "FailedRecordsCount": 1,
    "ImportDestination": {
        "SuppressionListDestination": {
            "SuppressionListImportAction": "PUT"
```

```
        }
    },
    "CompletedTimestamp": "2020-08-12T17:06:42Z"
}
```

So rufen Sie Informationen über einen Importauftrag für das Konto mit der SES-Konsole ab:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. Wählen Sie in der Suppression list (Unterdrückungsliste) die Option Bulk actions (Massenaktionen) aus.
4. Alle Importaufträge werden im Feld Bulk actions (Massenaktionen) als Tabelle zusammen mit Importtyp, Status und Datum aufgelistet.
5. Um Auftragsdetails anzuzeigen, wählen Sie die Auftrags-ID aus und die folgenden Bereiche werden angezeigt:

    a. Massenaktionsstatus: zeigt den Gesamtstatus der Aufträge, die Uhrzeit und das Datum, an dem sie abgeschlossen wurden an, wie viele Datensätze importiert wurden und die Anzahl aller Datensätze, die nicht erfolgreich importiert wurden.

    b. Details zur Massenaktion: zeigt die Auftrags-ID an, unabhängig davon, ob sie zum Hinzufügen oder Entfernen von Adressen verwendet wurde, ob das Dateiformat JSON oder CSV war, den URI des Amazon-S3-Buckets, in dem die Massendatei gespeichert wurde, sowie Uhrzeit und Datum, an dem die Massenaktion erstellt wurde.

Deaktivieren der Unterdrückungsliste auf Kontoebene von Amazon SES

Sie können den PutAccountSuppressionAttributesVorgang in der SES-API v2 verwenden, um Ihre Sperrliste auf Kontoebene effektiv zu deaktivieren, indem Sie die Werte aus dem `suppressed-reasons` Attribut entfernen.

Um Ihre Unterdrückungsliste auf Kontoebene zu deaktivieren, verwenden Sie den AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 put-account-suppression-attributes --suppressed-reasons
```

So deaktivieren Sie mit der SES-Konsole Ihre Unterdrückungsliste auf Kontoebene:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Suppression list (Unterdrückungsliste) aus.
3. Wählen Sie in Account-level settings (Einstellungen auf Kontoebene), Edit (Bearbeiten) aus.
4. Deaktivieren Sie in der Suppression list (Unterdrückungsliste) das Kontrollkästchen Enabled (Aktiviert).
5. Wählen Sie Änderungen speichern aus.

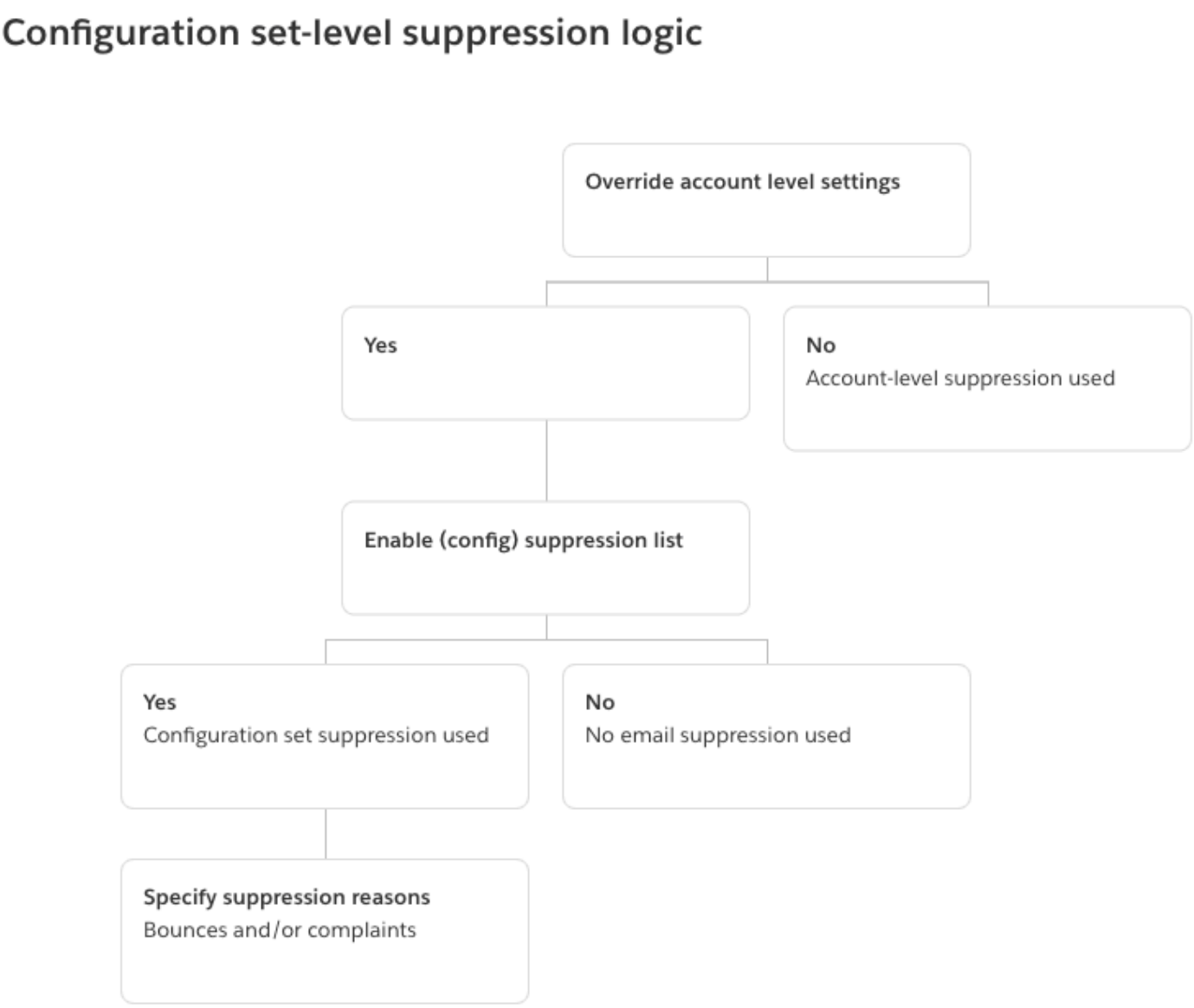
Verwenden der Unterdrückung auf Konfigurationssatzebene zum Überschreiben Ihrer Unterdrückungsliste auf Kontoebene

Während die Unterdrückungsliste auf Kontoebene für Ihr gesamtes Konto festgelegt ist, können Sie sie separat für verschiedene Konfigurationssätze anpassen, indem Sie sie mit der Unterdrückung auf Konfigurationssatzebene überschreiben. Diese feinere Granularität ermöglicht die Verwendung benutzerdefinierter Unterdrückungseinstellungen für verschiedene E-Mail-Versandgruppen, die Sie ihren eigenen Konfigurationssätzen zugewiesen haben. Angenommen, Ihre Unterdrückungsliste auf Kontoebene ist so konfiguriert, dass sowohl Unzustellbarkeits- als auch Beschwerdeadressen hinzugefügt werden. Sie haben jedoch eine bestimmte E-Mail-Demografie in einem Konfigurationssatz definiert, für die nur Beschwerdeadressen hinzugefügt werden sollen. Dies würden Sie erreichen, indem Sie die Unterdrückungsüberschreibungen dieses Konfigurationssatzes aktivieren, sodass E-Mail-Adressen nur für Beschwerden (nicht für Unzustellbarkeit und Beschwerden, wie sie in Ihrer Unterdrückungsliste auf Kontoebene festgelegt sind) aus E-Mails, die mit diesem Konfigurationssatz gesendet wurden, Ihrer Unterdrückungsliste auf Kontoebene hinzugefügt werden.

Bei der Unterdrückung auf Konfigurationssatzebene gibt es verschiedene Ebenen zum Überschreiben der Unterdrückung auf Kontoebene, einschließlich der Verwendung überhaupt keiner Unterdrückung. Zum besseren Verständnis dieser verschiedenen Unterdrückungsebenen, die in den folgenden Konsolenverfahren festgelegt werden können, modelliert die folgende Beziehungskarte den Satz von Entscheidungen, die Sie für das Aktivieren oder Deaktivieren verschiedener Überschreibungsebenen treffen können, die je nach Kombination zur Implementierung von drei verschiedenen Unterdrückungsstufen verwendet werden können:

- No overrides (default) (Keine Überschreibungen (Standard)) – Der Konfigurationssatz verwendet die Einstellungen für Ihre Unterdrückungsliste auf Kontoebene.
- Override account level settings (Einstellungen auf Kontoebene überschreiben) – Dies negiert alle Einstellungen für die Unterdrückungsliste auf Kontoebene. E-Mails, die mit diesem Konfigurationssatz gesendet werden, verwenden überhaupt keine Unterdrückungseinstellungen.
- Override account level settings with configuration set-level suppression enabled (Einstellungen auf Kontoebene mit aktivierter Unterdrückung auf Konfigurationssatzebene überschreiben) – E-Mails, die mit diesem Konfigurationssatz gesendet werden, verwenden nur die Unterdrückungsbedingungen, die Sie dafür aktiviert haben (Unzustellbarkeiten, Beschwerden oder beides). Ganz gleich, welche Einstellungen für die Unterdrückungsliste auf Kontoebene festgelegt wurden: Sie werden überschrieben.

> **Note**
>
> Für alle Unterdrückungsbedingungen, die nicht auf der Ebene der Konfigurationssätze angegeben sind, wird das Unterdrückungsverhalten auf die globale Unterdrückungsliste zurückgegriffen, da die Einstellungen auf Kontoebene überschrieben wurden.



Beachten Sie, dass es sich bei der Unterdrückung auf Konfigurationssatzebene um keine wirkliche Unterdrückungsliste handelt. Es ist vielmehr ein Verfahren zum Überschreiben Ihrer Unterdrückungsliste auf Kontoebene mit benutzerdefinierten Unterdrückungseinstellungen, die in einem Konfigurationssatz definiert sind. Dies bedeutet, dass jede E-Mail, die mit diesem Konfigurationssatz gesendet wird, nur ihre eigenen Unterdrückungseinstellungen verwendet und alle Unterdrückungseinstellungen auf Kontoebene ignoriert. Anders ausgedrückt: Die Unterdrückung auf Konfigurationssatzebene interagiert mit Ihrer Unterdrückungsliste auf Kontoebene, indem sie einfach die Unterdrückungsgründe ändert (überschreibt), die bestimmen, welche E-Mail-Adressen Ihrer Unterdrückungsliste auf Kontoebene hinzugefügt werden.

Aktiviereung der Unterdrückung auf Satzebene auf Konfigurationseinstellung

So aktivieren Sie die Unterdrückung auf Konfigurationsebene mit der neuen Amazon-SES-Konsole:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich unter Configuration (Konfiguration) Configuration sets (Konfigurationssätze) aus.
3. Wählen Sie unter Configuration sets (Konfigurationssätze) den Namen des Konfigurationssatzes aus, den Sie mit benutzerdefinierter Unterdrückung konfigurieren möchten.
4. Wählen Sie im Bereich Suppression list options (Optionen der Unterdrückungsliste) die Option Edit (Bearbeiten) aus.
5. Der Abschnitt Suppression list options (Unterdrückungslistenoptionen) enthält eine Entscheidungsgruppe zum Definieren einer benutzerdefinierten Unterdrückung, beginnend mit der Option, diese Konfiguration zu verwenden, um Ihre Unterdrückung auf Kontoebene zu überschreiben. Die Logik-Map für die Unterdrückung auf Satzebene hilft Ihnen, die Auswirkungen der Überschreibungskombinationen zu verstehen. Diese mehrschichtige Auswahl an Überschreibungen kann kombiniert werden, um drei verschiedene Unterdrückungsebenen zu implementieren:

   a. Verwenden Sie Unterdrückung auf Kontoebene: Überschreiben Sie Ihre Unterdrückung auf Kontoebene nicht und implementieren Sie keine Unterdrückung auf Konfigurationssatzebene. Grundsätzlich verwendet jede E-Mail, die mit diesem Konfigurationssatz gesendet wird, nur Ihre Unterdrückung auf Kontoebene. So gehen Sie vor:

      - Deaktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

   b. Verwenden Sie keine Unterdrückung: Überschreiben Sie die Unterdrückung auf Kontoebene, ohne die Unterdrückung auf Konfigurationssatzebene zu aktivieren. Dies bedeutet, dass alle mit diesem Konfigurationssatz gesendeten E-Mails keine Unterdrückung auf Kontoebene verwenden – mit anderen Worten, jede Unterdrückung wird aufgehoben. So gehen Sie vor:

i. Aktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

ii. Deaktivieren Sie in der Suppression list (Unterdrückungsliste) das Kontrollkästchen Enabled (Aktiviert).

c. Use configuration set-level suppression (Unterdrückung auf Konfigurationssatzebene verwenden): Überschreiben Sie Ihre Unterdrückungsliste auf Kontoebene mit benutzerdefinierten Unterdrückungseinstellungen, die in diesem Konfigurationssatz definiert sind. Dies bedeutet, dass jede E-Mail, die mit diesem Konfigurationssatz gesendet wird, nur ihre eigenen Unterdrückungseinstellungen verwendet und alle Unterdrückungseinstellungen auf Kontoebene ignoriert. So gehen Sie vor:

i. Aktivieren Sie in den Suppression list settings (Unterdrückungslisteneinstellungen), dass das Kontrollkästchen Override account level settings (Einstellungen auf Kontoebene überschreiben).

ii. Wählen Sie in der Suppression list (Unterdrückungsliste) Enabled (Aktiviert) aus.

iii. Wählen Sie in Specify the reason(s)... (Geben Sie den Grund(e) an ...) einen der Unterdrückungsgründe für diese zu verwendende Konfiguration aus.

6. Wählen Sie Save Changes (Änderungen speichern).

Verwenden von Listenverwaltung

Amazon SES bietet Funktionen zur Listenverwaltung, d. h. Kunden können ihre eigenen Mailinglisten, die als Kontaktlisten bezeichnet werden, verwalten. Eine Kontaktliste ist eine Liste, mit der Sie alle Ihre Kontakte speichern können, die ein bestimmtes Thema oder bestimmte Themen abonniert haben. Ein Kontakt ist ein Endbenutzer, der Ihre E-Mails erhält. Ein Thema ist eine Interessengruppe, ein Design oder ein Label innerhalb einer Liste. Listen können mehrere Themen haben.

Durch die Verwendung der `ListContacts`-Operation in der Amazon SES API v2 können Sie eine Liste aller Kontakte abrufen, die ein bestimmtes Thema abonniert haben, an die Sie mit der `SendEmail`-Operation E-Mails senden können.

Weitere Informationen zu Jahresabonnements finden Sie unter Abonnementverwaltung.

Übersicht über die Verwaltung von

Sie sollten die folgenden Faktoren berücksichtigen, wenn Sie die globale Unterdrückungsliste verwenden:

- Sie können Listenthemen beim Erstellen der Liste angeben.
- Pro ist nur eine Kontaktliste zulässig AWS-Konto.
- Eine Liste kann maximal 20 Themen haben.
- Sie können eine vorhandene Kontaktliste aktualisieren. Dazu gehören das Hinzufügen neuer Themen zur Liste, das Hinzufügen oder Löschen von Kontakten aus einer Liste und das Aktualisieren von Kontakteinstellungen für eine Liste oder ein Thema.
- Sie können Topic-Metadaten aktualisieren, z. B. den Anzeigenamen oder die Beschreibung des Themas.
- Sie können eine Liste der Kontakte in einer Kontaktliste, Kontakte, die ein Thema abonniert haben, Kontakte, die von einem Thema abgemeldet wurden, sowie Kontakte abrufen, die von allen Themen in der Liste abgemeldet wurden.
- Sie können Ihre vorhandenen Kontaktlisten mithilfe der `CreateImportJob`API in SES importieren.
- SES gibt ein Bounce-Event für eine Nachricht aus, die an einen Kontakt auf Ihrer Kontaktliste gesendet wird, der sich nicht abonniert hat. Weitere Informationen finden Sie unter Abonnementverwaltung.
- Jedem Kontakt kann zugeordnete Attribute aufweisen, mit denen Sie Informationen zu diesem Kontakt speichern können.

Konfigurieren der Listenverwaltung

Sie können zur Konfiguration von Listenverwaltungsfunktionen wie folgt verwenden: Eine vollständige Liste der Kontaktlisten und -operationen finden Sie imAmazon SES API v2-Referenzaus.

Erstellen von Gesprächslisten

Sie können den `CreateContactList`Vorgang in der SES-API v2 verwenden, um eine Kontaktliste zu erstellen. Sie können diese Einstellung schnell und einfach konfigurieren, indem Sie die AWS CLI verwenden. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Um eine Kontaktliste mit dem zu erstellen AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 create-contact-list --cli-input-json file://CONTACT-LIST-JSON
```

Ersetzen Sie es im vorherigen Befehl *CONTACT-LIST-JSON* durch den Pfad zu Ihrer JSON-Datei für Ihre `CreateContactList`Anfrage.

Eine Beispielhafte `CreateContactList`-Eingabe-JSON-Datei für die Anforderung ist wie folgt:

```
{
    "ContactListName": "ExampleContactListName",
    "Description": "Creating a contact list example",
    "Topics": [
     {
         "TopicName": "Sports",
         "DisplayName": "Sports Newsletter",
         "Description": "Sign up for our free newsletter to receive updates on all
 sports.",
         "DefaultSubscriptionStatus": "OPT_OUT"
     },
     {
         "TopicName": "Cycling",
         "DisplayName": "Cycling newsletter",
         "Description": "Never miss a cycling update by subscribing to our
 newsletter.",
         "DefaultSubscriptionStatus": "OPT_IN"
     },
     {
         "TopicName": "NewProducts",
         "DisplayName": "New products",
         "Description": "Hear about new products by subscribing to this mailing
 list.",
         "DefaultSubscriptionStatus": "OPT_IN"
     },
     {
         "TopicName": "DailyUpdates",
         "DisplayName": "Daily updates",
         "Description": "Start your day with sport updates, Monday through
 Friday.",
         "DefaultSubscriptionStatus": "OPT_OUT"
```

```
     }
    ]
}
```

So erstellen Sie einen Kontakt

Sie können den `CreateContact`Vorgang in der SES-API v2 verwenden, um einen Kontakt zu erstellen. Sie können diese Einstellung schnell und einfach konfigurieren, indem Sie die AWS CLI verwenden. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Um einen Kontakt mit dem zu erstellen AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws sesv2 create-contact --cli-input-json file://CONTACT-JSON
  ```

  Ersetzen Sie es im vorherigen Befehl *CONTACT-JSON* durch den Pfad zu Ihrer JSON-Datei für Ihre `CreateContact`Anfrage.

  Eine Beispielhafte `CreateContact`-Eingabe-JSON-Datei für die Anforderung ist wie folgt:

  ```
  {
      "ContactListName": "ExampleContactListName",
      "EmailAddress": "example@amazon.com",
      "UnsubscribeAll": false,
      "TopicPreferences": [
          {
              "TopicName": "Sports",
              "SubscriptionStatus": "OPT_IN"
          }
      ],
      "AttributesData": "{\"Name\": \"John\", \"Location\": \"Seattle\"}"
  }
  ```

  Im obigen Beispiel zeigt ein `UnsubscribeAll`-Wert von `false`an, dass sich der Kontakt nicht von allen Themen abgemeldet hat, wobei der Wert `true` bedeuten würde, dass sich der Kontakt von allen Themen abgemeldet hat.

`TopicPreferences` enthält Informationen zum Abonnementstatus des Kontakts für Themen. Im vorangegangenen Beispiel hat sich der Kontakt für das Thema „Sport“ entschieden und erhält alle E-Mails zum Thema „Sport“.

`AttributesData` ist ein JSON-Feld, in dem Sie beliebige Metadaten über unseren Kontakt einfügen können. Es muss ein gültiges JSON-Objekt sein.

Massenimport von Kontakten in Ihre Kontaktliste

Sie können Adressen manuell in großen Mengen hinzufügen, indem Sie zuerst Ihre Kontakte in ein Amazon S3 S3-Objekt hochladen und anschließend den `CreateImportJob`Vorgang in der SES API v2 oder die SES-Konsole verwenden. Weitere Informationen finden Sie unter Hinzufügen von E-Mail-Adressen in Ihrer Unterdrückungsliste auf Kontoebene.

Sie sollten eine Kontaktliste erstellen, bevor Sie Ihre Kontakte importieren.

> **Note**
>
> Sie können einer Kontaktliste bis zu 1 Million Kontakte pro Person ImportJob hinzufügen.

Führen Sie die folgenden Schritte aus, um der Kontaktliste mehrere Kontakte hinzuzufügen.

- Laden Sie Ihre Kontakte in ein Amazon S3 Objekt im CSV- oder JSON-Format hoch.

  CSV-Format

  Die erste Zeile der Datei, die in Amazon S3 hochgeladen wird, sollte eine Kopfzeile sein.

  Das `topicPreferences`-Objekt muss für das CSV-Format abgeflacht werden. Jedes Thema in den `topicPreferences` hat ein separates Kopfzeilenfeld.

  CSV-Format Beispiel für das Hinzufügen von Kontakten in einem Massenformat zu einer Kontaktliste:

```
emailAddress,unsubscribeAll,attributesData,topicPreferences.Sports,topicPreferences.Cycling
example1@amazon.com,false,{"Name": "John"},OPT_IN,OPT_OUT
example2@amazon.com,true,,OPT_OUT,OPT_OUT
```

JSON-Format

Nur durch Zeilenumbrüche getrennte JSON-Dateien werden unterstützt. In diesem Format ist jede Zeile ein vollständiges JSON-Objekt mit den Informationen eines Kontakts.

Beispiel für das JSON-Format zum Hinzufügen von Kontakten in einer Kontaktliste:

```
{
     "emailAddress": "example1@amazon.com",
     "unsubscribeAll": false,
     "attributesData": "{\"Name\":\"John\"}",
     "topicPreferences": [
      {
          "topicName": "Sports",
          "subscriptionStatus": "OPT_IN"
      },
      {
          "topicName": "Cycling",
          "subscriptionStatus": "OPT_OUT"
      }
     ]
}
{
     "emailAddress": "example2@amazon.com",
     "unsubscribeAll": true,
     "topicPreferences": [
      {
          "topicName": "Sports",
          "subscriptionStatus": "OPT_OUT"
      },
      {
          "topicName": "Cycling",
          "subscriptionStatus": "OPT_OUT"
      }
     ]
}
```

Ersetzen Sie in den vorherigen Beispielen *example1@amazon.com* und *example2@amazon.com* durch die E-Mail-Adressen, die Sie der Kontaktliste hinzufügen möchten. Ersetzen Sie die `attributesData`-Werte durch die für den Kontakt spezifischen Werte. Ersetzen Sie außerdem *Sports* und *Cycling* durch `topicName` das, was für Ihren Kontakt gilt. Zulässig `topicPreferences` sind *OPT_IN* und*OPT_OUT*.

Die folgenden Attribute werden unterstützt, wenn Sie Ihre Kontakte in ein Amazon S3 Objekt im CSV- oder JSON-Format hochladen:

Attribut	Description
`emailAddress`	Die E-Mail-Adresse des Kontakts. Dieser ist ein obligatorisches Feld.
`unsubscribeAll`	Ein boolescher Wertstatus, der angibt, ob der Kontakt von allen Themen der Kontaktliste abgemeldet wird.
`topicPreferences`	Die Präferenzen des Kontakts für die Opt-In oder Opt-Out von Themen.
`attributesData`	Die Attributdaten, die einem Kontakt zugeordnet sind.

- Erteilen Sie SES Berechtigung, das Amazon S3 Objekt zu lesen.

  Bei Anwendung auf einen Amazon-S3-Bucket erteilt die folgenden Richtlinie SES die Berechtigung zum Schreiben von Daten in diesen Bucket. Weitere Informationen zu Bucket-Richtlinien für Amazon S3 finden Sie unter Verwenden von Bucket-Richtlinien und Benutzerrichtlinien im Entwicklerhandbuch zu Amazon Simple Storage Service.

- Erteilen Sie SES die Erlaubnis, Ihren AWS KMS Schlüssel zu verwenden.

  Wenn das Amazon S3 S3-Objekt mit einem AWS KMS Schlüssel verschlüsselt ist, müssen Sie Amazon SES die Erlaubnis zur Verwendung des KMS-Schlüssels erteilen. SES kann nur die Berechtigung von einem vom Kunden verwalteten Schlüssel erhalten, nicht von einem standardmäßigen KMS-Schlüssel. Sie müssen SES die Erlaubnis zur Verwendung des vom Kunden verwalteten Schlüssels erteilen, indem Sie der Richtlinie für den Schlüssel eine Erklärung hinzufügen.

Fügen Sie die folgende Richtlinienanweisung in die Schlüsselrichtlinie ein, um SES zu erlauben, Ihren vom Kunden verwalteten Schlüssel zu verwenden.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Verwenden Sie den `CreateImportJob`Vorgang in der SES-API v2.

> **Note**
>
> Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zur Installation und Konfiguration von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Geben Sie in der Befehlszeile den folgenden Befehl ein: Ersetzen *`s3bucket`* Sie durch den Namen des Amazon S3 S3-Buckets und *`s3object`* durch den Namen des Amazon S3 S3-Objektnamens.

```
aws sesv2 create-import-job --import-destination
 ContactListDestination={ContactListName=ExampleContactListName,ContactListImportAction=PUT}
 --import-data-source S3Url="s3://s3bucket/s3object",DataFormat=CSV
```

Exemplarische Vorgehensweise zur Listenverwaltung mit Beispielen

Die folgende exemplarische Vorgehensweise enthält Beispiele, wie Sie mit der Listenverwaltung Ihre Kontakte aufführen und `ListManagementOptions` nutzen können, um eine Kontaktliste und einen Themennamen in Ihrer E-Mail anzugeben und Abmeldelinks einzufügen.

1. Kontakte auflisten mit dem AWS CLI — Sie können den `ListContacts`Vorgang verwenden, um in Verbindung mit dem `SendEmail`Vorgang eine Liste all Ihrer Kontakte abzurufen, die ein bestimmtes Thema abonniert haben, sodass Sie ihnen E-Mails senden können.

   Geben Sie in der Befehlszeile folgenden Befehl ein:

   ```
   aws sesv2 list-contacts --cli-input-json file://LIST-CONTACTS-JSON
   ```

   Ersetzen Sie dies im vorherigen Befehl *`LIST-CONTACTS-JSON`* durch den Pfad zu Ihrer JSON-Datei für Ihre `ListContacts`Anfrage.

   Eine Beispielhafte `ListContacts`-Eingabe-JSON-Datei für die Anforderung ist wie folgt:

   ```
   {
       "ContactListName": "ExampleContactListName",
       "Filter": {
           "FilteredStatus": "OPT_IN",
           "TopicFilter": {
               "TopicName": "Cycling",
               "UseDefaultIfPreferenceUnavailable": true
           }
       },
       "PageSize": 50
   }
   ```

   `FilteredStatus` zeigt den Abonnementstatus an, auf den Sie filtern möchten, der entweder `OPT_IN`oder `OPT_OUT` ist.

   `TopicFilter` ist ein optionaler Filter, der angibt, für welches Thema Sie Ergebnisse wünschen. Im obigen Beispiel ist das „Radfahren“.

   `UseDefaultIfPreferenceUnavailable` kann den Wert `true` oder `false` aufweisen. Wenn`true`, wird die Standardeinstellung des Themas verwendet, wenn der Kontakt keine explizite Präferenz für ein Thema hat. Wenn`false`auswählen, werden nur Kontakte mit einer explizit festgelegten Voreinstellung für die Filterung berücksichtigt.

2. E-Mail mit **`ListManagementOptions`** aktiviert senden – nachdem Sie die Kontakte in Ihrer Liste mit der oben genannten `ListContacts`-Operation aufgelistet haben, können Sie mit der `SendEmail`-Operation E-Mails an jeden Ihrer Kontakte senden, indem Sie den

`ListManagementOptions`-Header verwenden, um Ihre Kontaktliste und Ihren Themennamen anzugeben.

Wenn Sie `ListManagementOptions` mit der `SendEmail`-Operation verwenden möchten, schließen Sie `contactListName` und `topicName` zu der die E-Mail gehört (der `topicName` ist optional) ein:

```
ListManagementOptions:
    String contactListName
    String topicName
```

Wenn Sie `ListManagementOptions` in Ihre `SendEmail`-Anfrage an eine Empfänger-E-Mail-Adresse einfügen, die nicht in Ihrer Kontaktliste enthalten ist, wird automatisch ein Kontakt in Ihrer Liste erstellt.

SES gibt ein Bounce-Ereignis für eine Nachricht aus, die an einen Kontakt auf Ihrer Kontaktliste gesendet wird, der sich nicht angemeldet hat. Das bedeutet, dass Sie Ihre `SendEmail` Anfragen nicht aktualisieren müssen, um zu vermeiden, dass sie an Kontakte gesendet werden, die sich abgemeldet haben.

3. Geben Sie den Speicherort für Ihre Abmeldelinks an — Wenn Sie diese Option verwenden, haben `ListManagementOptions`Sie die Möglichkeit, SES zu ermöglichen, Ihrer E-Mail Fußzeilenlinks zum Abbestellen hinzuzufügen. Verwenden Sie dazu den `{{amazonSESUnsubscribeUrl}}` Platzhalter, um anzugeben, wo SES die Abmelde-URL einfügen muss. Der Austausch von Platzhaltern wird nur für HTML- und TEXT-Typen unterstützt. Sie können den Platzhalter maximal zwei Mal einschließen. Bei mehrfacher Verwendung werden nur die ersten beiden Vorkommen ersetzt. Weitere Informationen finden Sie unter Abonnementverwaltung.

   Sie können aber auch den `X-SES-LIST-MANAGEMENT-OPTIONS`-Header verwenden, um beim Senden von E-Mails über die SMTP-Schnittstelle eine Liste und einen Themennamen anzugeben.

   Um beim Senden von E-Mails über die SMTP-Schnittstelle eine Liste und ein Thema anzugeben, fügen Sie der Nachricht den folgenden E-Mail-Header hinzu:

   ```
   X-SES-LIST-MANAGEMENT-OPTIONS: {contactListName}; topic={topicName}
   ```

Abonnementverwaltung

Amazon SES bietet eine Abonnementverwaltungsfunktion, bei der Amazon SES automatisch die Abmeldelinks in jeder ausgehenden E-Mail aktiviert, wenn Sie `contactListName` und `topicName` in `ListManagementOptions` im Feld in der `SendEmail`-Operationsanforderung angeben.

Wenn sich ein Kontakt von einem bestimmten Thema oder einer Liste abmeldet, lässt Amazon SES zukünftig keine E-Mail an den Kontakt zu diesem Thema oder dieser Liste zu.

> **Note**
>
> - Die Amazon SES SES-Abonnementverwaltung unterstützt die Anforderungen an Massenabsender, die von vielen E-Mail-Dienstanbietern durchgesetzt werden. Weitere Informationen finden Sie in Abschnitt 2 in Überblick über Änderungen an Massensendern.
> - Abonnementverwaltung ist für diejenigen verfügbar, dieEasy DKIM in Amazon SES, aber es ist nicht möglich, dass Amazon SES die Abmeldelinks zu Ihrer E-Mail für Absender hinzufügen, die E-Mails selbst signieren, bevor Sie Amazon SES anrufen.

Weitere Informationen über die Listenverwaltung und deren Verwendung, einschließlich des Abrufs einer Liste aller Kontakte, die ein bestimmtes Thema abonniert haben, finden Sie unter Verwenden von Listenverwaltung.

Abonnementverwaltung

Sie sollten die folgenden Faktoren berücksichtigen, wenn Sie Abonnementverwaltung verwenden:

- Die Abonnementverwaltung wird vollständig von Amazon SES verwaltet. Dies bedeutet, dass Amazon SES E-Mails und Anfragen von der Abmeldewebseite erhält und die Einstellungen des Kontakts in Ihrer Liste aktualisiert. Sie können Abmeldebenachrichtigungen mit Konfigurationsset-Benachrichtigungen erhalten. Weitere Informationen zu Konfigurationssätzen finden Sie unter Verwenden von Amazon SES-Konfigurationssätzen im.
- Sie müssen die Kontaktliste angeben, während Sie die E-Mail senden. Die Abonnementverwaltung über die `List-Unsubscribe`-Kopf- und `ListManagementOptions`-Fußzeilenlinks wird entsprechend behandelt.

- Amazon SES fügt Unterstützung für die `List-Unsubscribe`-Header-Standards hinzu, die es E-Mail-Clients und Posteingangsanbietern ermöglichen, einen Abmelde-Link oben in der E-Mail anzuzeigen, wenn sie diese unterstützen – nicht alle Serviceanbieter unterstützten diese Header.
- `List-Unsubscribe`-Header folgen folgendem Verhalten:
  - Wenn ein Kontakt in einer E-Mail auf den Abmeldelink klickt, in der sowohl die Kontaktliste als auch das Thema angegeben ist, wird der Kontakt nur von diesem bestimmten Thema abgemeldet.
  - Wenn das Thema nicht angegeben ist, wird der Kontakt von allen Themen in der Liste abgemeldet.
- Kontakte werden zu einer Zielseite zum Abmelden weitergeleitet, wenn sie in der E-Mail-Fußzeile auf einen Abmelde-Link klicken.
- Die Zielseite zum Abmelden gibt Kontakten die Möglichkeit, ihre Präferenzen zu aktualisieren.`OPT_IN`oder`OPT_OUT`, für alle Themen in einer bestimmten Liste. Die Zielseite bietet auch die Möglichkeit, sich von allen Themen in der Liste abzumelden.
- Bei Verwendung von `ListManagementOptions` müssen Sie den `{{amazonSESUnsubscribeUrl}}`-Platzhalter in Ihre E-Mails einfügen, um anzugeben, wo Amazon SES die Abmelde-URL einfügen muss. Sie können den Platzhalter maximal zwei Mal einschließen. Bei mehrfacher Verwendung werden nur die ersten beiden Vorkommen ersetzt.
- Die `List-Unsubscribe`-Kopf- und `ListManagementOptions`-Fußzeilenlinks werden nur hinzugefügt, wenn die E-Mail an einen einzelnen Empfänger gesendet wird.
- Bei Transaktions-E-Mails, bei denen Sie nicht möchten, dass Kontakte sich abmelden können, können Sie das Feld `ListManagementOptions` mit Ihrer `SendEmail`-Anfrage weglassen.

Überlegungen zur Abmeldung von Kopfdaten

Die Abonnementverwaltung über einen Abmeldelink ist aktiviert, wenn die E-Mail die folgenden Header enthält:

`List-Unsubscribe`

`List-Unsubscribe-Post`

Wenn Sie das Abonnementverwaltung von Amazon SES verwenden, `ListManagementOptions`, setzt Amazon SES diese Header außer Kraft, wenn sie in der E-Mail vorhanden sind.

Empfängern, die sich abmelden, indem sie auf den Link klicken, der von diesen Headern erstellt wurde, wird je nach E-Mail-Client oder Posteingangs eine andere Erfahrung angezeigt, da einige Anbieter die `List-Unsubscribe`- und `List-Unsubscribe-Post`-Header nicht erkennen. Für E-Mails, die mit solchen Anbietern an Empfänger gesendet werden, wird der Link zum Abbestellen nicht angezeigt.

Empfänger, deren E-Mail-Client diese Header erkennt, sehen den Link „Abmelden“ und können sich über den Link abmelden, haben jedoch nicht die Möglichkeit zu wählen, von welchen Themen sie sich abmelden und werden einfach von dem Thema abgemeldet, an das die E-Mail gesendet wurde.

Weitere Informationen zu `List-Unsubscribe`-Headern finden Sie unter RFC 2369. Informationen zu den `List-Unsubscribe-Post`-Headern finden Sie unter RFC 8058.

> **Note**
>
> Amazon SES unterstützt die Abmeldung mit einem Klick gemäß den Anforderungen für Massenabsender, die von vielen E-Mail-Dienstanbietern vorgeschrieben sind. Weitere Informationen finden Sie unter Verwenden der One-Click-Abmeldung mit Amazon SES.

Hinzufügen eines Link zum Abmelden der Fußzeile

Dazu benötigen Sie den`{{amazonSESUnsubscribeUrl}}`-Platzhalter in E-Mails mit Vorlagen und ohne Vorlagen, um anzugeben, wo Amazon SES die Abmelde-URL einfügen muss.

Der Austausch von Platzhaltern wird nur für HTML- und TEXT-Typen unterstützt.

Sie können den Platzhalter maximal zwei Mal einschließen. Bei mehrfacher Verwendung werden nur die ersten beiden Vorkommen ersetzt.

> **Note**
>
> Der `{{amazonSESUnsubscribeUrl}}` Platzhalter kann nur verwendet werden, wenn `ListManagementOptions`er bei der `SendEmail`Operation als Header oder X-SES-LIST-MANAGEMENT -OPTIONS bei der Verwendung der SMTP-Schnittstelle als Header angegeben wurde. (Nicht zu verwechseln mit den `List-Unsubscribe`- oder `List-Unsubscribe-Post`-Headern, die nicht von `ListManagementOptions` abhängig sind und alleine benutzt werden können.)

Überwachen Ihrer Amazon SES-Sendeaktivität

Amazon SES stellt Methoden für die Überwachung Ihrer Sendeaktivität mithilfe von Ereignissen, Metriken und Statistiken bereit. Ein Ereignis passiert im Zusammenhang mit Ihrer Sendeaktivität, von der Sie angegeben haben, dass sie als Metrik verfolgt werden soll. Eine Metrik stellt eine zeitlich angeordnete Gruppe von Datenpunkten, die die Werte eines überwachten Ereignistyps darstellen, dar, der Statistiken erstellt. Statistiken sind Metrikdaten-Aggregationen für einen bestimmten Zeitraum, einschließlich bis heute.

Diese Überwachungsmethoden helfen Ihnen, wichtige Maßnahmen wie die Unzustellbarkeits-, Beschwerde- und Ablehnungsraten Ihres Kontos im Auge zu behalten. Übermäßig hohe Unzustellbarkeits- und Beschwerdequoten können dazu führen, dass Sie keine E-Mails mehr mit SES senden können. Diese Methoden können auch verwendet werden, um die Preise zu messen, zu denen Ihre Kunden mit den von Ihnen gesendeten E-Mails interagieren, indem Sie Ihre gesamten Öffnungs- und Klickraten unter Verwendung von Ereignisveröffentlichungen und benutzerdefinierten Domänen, die mit Konfigurationssätzen verknüpft sind, identifizieren – siehe Konfigurieren von benutzerdefinierten Domänen zur Verarbeitung der Öffnungs- und Klicknachverfolgung.

Der erste Schritt beim Einrichten der Überwachung besteht darin, die Arten von E-Mail-Ereignissen im Zusammenhang mit Ihrer Sendeaktivität zu identifizieren, die Sie mit SES messen und überwachen möchten. Sie können die folgenden Ereignistypen auswählen, die in SES überwacht werden sollen:

- Send (Senden) – die Sendeanfrage war erfolgreich und Amazon SES versucht, dem E-Mail-Server des Empfängers die Nachricht zuzustellen. (Wenn eine Unterdrückung auf Kontoebene oder eine globale Unterdrückung verwendet wird, zählt SES sie weiterhin als Senden, aber die Zustellung wird unterdrückt.)
- RenderingFailure— Die E-Mail wurde aufgrund eines Problems beim Rendern der Vorlage nicht gesendet. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail-Vorlage mithilfe der `SendTemplatedEmail`- oder `SendBulkTemplatedEmail`-API-Operationen senden.
- Rejects (Ablehnungen) – Amazon SES hat die E-Mail akzeptiert, aber festgestellt, dass sie einen Virus enthielt und nicht versucht hat, ihn an den Mail-Server des Empfängers zu übermitteln.
- Delivery (Zustellung) – Amazon SES hat die E-Mail erfolgreich an den Mail-Server des Empfängers übermittelt.

- Bounce – eine permanente Unzustellbarkeit, sodass die E-Mail vom E-Mail-Server des Empfängers dauerhaft abgelehnt wurde. (Soft Bounces sind nur enthalten, wenn SES nicht mehr versucht, die E-Mail zuzustellen. Im Allgemeinen deuten diese Soft Bounces auf einen Zustellungsfehler hin, obwohl in einigen Fällen ein Soft Bounce auch dann zurückgegeben werden kann, wenn die E-Mail den Posteingang des Empfängers erfolgreich erreicht hat. Dies tritt normalerweise auf, wenn der Empfänger eine out-of-office automatische Antwort sendet. In diesem AWS re:POST-Artikel erfährst du mehr über Soft Bounces.)
- Complaint (Beschwerde) – die E-Mail wurde erfolgreich an den E-Mail-Server des Empfängers gesendet, der Empfänger hat sie jedoch als Spam markiert.
- DeliveryDelay— Die E-Mail konnte nicht an den Mailserver des Empfängers zugestellt werden, da ein vorübergehendes Problem aufgetreten ist. Verzögerungen bei der Zustellung können, z. B. auftreten, wenn der Posteingang des Empfängers voll ist oder der empfangende E-Mail-Server ein vorübergehendes Problem aufweist.
- Subscription (Abonnement) – die E-Mail wurde erfolgreich zugestellt, aber der Empfänger hat die Abonnementeinstellungen aktualisiert, indem er auf `List-Unsubscribe` in der E-Mail-Kopfzeile oder auf den `Unsubscribe`-Link in der Fußzeile geklickt hat.
- Open (Geöffnet) – der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
- Click (Klick) – der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.

Sie können E-Mail-Sendeereignisse auf verschiedene Arten überwachen. Welche Methode Sie wählen, hängt von der Art des Ereignisses ab, das Sie überwachen möchten, von der Granularität und dem Detaillierungsgrad, mit dem Sie es überwachen möchten, und vom Ort, an dem SES die Daten veröffentlichen soll. Sie müssen entweder Feedback-Benachrichtigungen oder Ereignisveröffentlichung verwenden, um Unzustellbarkeits- und Beschwerdeereignisse nachzuverfolgen. Sie haben auch die Möglichkeit, mehrere Überwachungsmethoden einzusetzen. In der folgenden Tabelle finden Sie die Merkmale der einzelnen Methoden.

Überwachungsmethode	Überwachbare Ereignisse	Datenzugriff erfolgt über	Detailgenauigkeit	Granularity
SES-Konsole	Kontozustand, gesendete E-Mails, verwendetes Kontingen	Konto-Dashboard-Seite in der SES-Konsole	Prozentsatz	Für das gesamte AWS Konto

Überwachungsmethode	Überwachbare Ereignisse	Datenzugriff erfolgt über	Detailgenauigkeit	Granularity
	t, erfolgreiche Sendeanfragen, Ablehnungen, Unzustellbarkeiten & Beschwerden (jüngste Geschichte bis zur aktuellen Reputation)			
SES-Konsole	Kontozustand, gesendete E-Mails, Unzustellbarkeiten & Beschwerden (aktuelle Reputation)	Seite mit Reputationsmetriken in der SES-Konsole	Nur berechnete Quoten	Für das gesamte AWS Konto
Virtueller Zustellbarkeitsmanager	Kontostatistiken, ISP, Sendeidentitäten, Konfigurationssätze, Versand, Zustellung, Beschwerden, vorübergehende und permanente Bounces, Öffnungen und Klicks, Zustellbarkeit und Reputation.	the section called “Dashboard”in der SES-Konsole the section called “Berater”in der SES-Konsole	Prozentsatz	Für das gesamte AWS Konto

Überwachungsmethode	Überwachbare Ereignisse	Datenzugriff erfolgt über	Detailgenauigkeit	Granularity
SIEHE API	Zustellungen, Unzustellbarkeiten, Beschwerden und Ablehnungen	`GetSendStatistics` API-Operation	Nur Zählung	Für das gesamte AWS Konto

Überwachungsmethode	Überwachbare Ereignisse	Datenzugriff erfolgt über	Detailgenauigkeit	Granularity
CloudWatch Amazon-Konsole	Sendungen, Lieferungen, Öffnungen, Klicks, Bounces, Absprungrate, Beschwerden, Reklamationsrate, Ablehnungen, Renderfehler und schwarze Liste. IPs	CloudWatch Konsole **Note** Einige Messwerte werden CloudWatch erst angezeigt, wenn das zugehörige Ereignis eintritt. Beispielsweise werden Bounce-Metriken CloudWatch erst in mindestens einer E-Mail angezeigt, in der Sie Bounces versenden, oder bis Sie	Nur Zählung	AWS Für das gesamte Konto

Überwachungsmethode	Überwachbare Ereignisse	Datenzugriff erfolgt über	Detailgenauigkeit	Granularity
		mithilfe des Mailbox-Simulators ein simuliertes Bounce-Ereignis generieren.		
Feedback-Benachrichtigungen	Zustellungen, Unzustellbarkeiten und Beschwerden	Amazon SNS-Benachrichtigung (Zustellungen, Unzustellbarkeiten und Beschwerden) oder E-Mail (nur Unzustellbarkeiten und Beschwerden) Siehe Einrichten von Ereignisbenachrichtigungen.	Details zu jedem Ereignis	Für das gesamte AWS Konto

Überwachungsmethode	Überwachbare Ereignisse	Datenzugriff erfolgt über	Detailgenauigkeit	Granularity
Event publishing (Ereignis veröffentlichung)	Fehler beim Senden, Zustellen, Klicken, Senden von Unzustellbarkeitsbenachrichtigungen, Beschweren, Ablehnen und Rendering.	Amazon CloudWatch oder Amazon Data Firehose oder per Amazon SNS SNS-Benachrichtigung — siehe. Überwachen des E-Mail-Versands mithilfe der Ereignisveröffentlichung (Es fallen zusätzliche Gebühren an, siehe Preis pro Metrik für.) CloudWatch	Details zu jedem Ereignis	Differenziert (basierend auf benutzerdefinierten E-Mail-Eigenschaften)

Überwachungsmethode	Überwachbare Ereignisse	Datenzugriff erfolgt über	Detailgenauigkeit	Granularity
Ereignisveröffentlichung unter Verwendung benutzerdefinierter Domänen, die Konfigurationssätze zugeordnet sind – Weitere Infos	Öffnen Sie Tracking und klicken Sie darauf.	Amazon CloudWatch oder Amazon Data Firehose oder per Amazon SNS SNS-Benachrichtigung. (Es fallen zusätzliche Gebühren an, siehe Preis pro Metrik für CloudWatch.)	Details zu jedem Ereignis.	Differenziert (basierend auf benutzerdefinierten E-Mail-Eigenschaften)

> **Note**
>
> Die anhand von E-Mail-Sendeereignissen gemessenen Metriken stimmen möglicherweise nicht mit Ihren Sendekontingenten überein. Diese Diskrepanz kann durch zurückgesendete und abgelehnte E-Mails oder durch die Verwendung des SES-Posteingangssimulators verursacht werden. Weitere Informationen darüber, wie Sie herausfinden können, wann die Grenze Ihrer Sendekontingente erreicht ist, finden Sie unter Überwachung Ihrer Sendekontingente.

Weitere Informationen zum Verwenden der einzelnen Überwachungsmethoden finden Sie in den folgenden Themen:

- Überwachen der Sendestatistiken mithilfe der Amazon-SES-Konsole
- Überwachen der Nutzungsstatistiken mit der API von Amazon SES
- Überwachen des E-Mail-Versands mithilfe der Amazon SES-Ereignisveröffentlichung

Überwachen der Sendestatistiken mithilfe der Amazon-SES-Konsole

Auf den Seiten Konto-Dashboard, Zuverlässigkeitsmetriken und SMTP-Einstellungen der Amazon-SES-Konsole können Sie Ihren gesamten E-Mail-Versand, die Nutzung, Statistiken, SMTP-Einstellungen, den allgemeinen Kontozustand und die Zuverlässigkeitsmetriken überwachen. In den folgenden Abschnitten werden die Metriken und Statistiken beschrieben, die jeweils auf diesen Konsolenseiten bereitgestellt werden.

Hinweis: Die beiden Konsolenseiten the section called “Konto-Dashboard” und the section called “Zuverlässigkeitsmetriken” enthalten zwar beide Unzustellbarkeits- und Beschwerdemetriken, doch es gibt einen subtilen Unterschied zwischen diesen Metriken für Unzustellbarkeits- und Beschwerderaten, wie nachfolgend erläutert:

- Konto-Dashboard-Seite – basierend auf dem ausgewählten Datumsbereich können Sie sehen, wie hoch die Unzustellbarkeits- und Beschwerderaten in der Vergangenheit waren, die den metrischen Fortschritt der Änderungen bis zur gegenwärtigen Zeit zeigen.
- Seite mit Reputationskennzahlen — Absprungs- und Beschwerdequoten basieren auf dem letzten Datenpunkt, den Sie aus der Berechnung Ihres historischen Gesamtdurchschnitts auf hohem Niveau erhalten haben (dies sollte nicht mit Ihrer regulären bounce/complaint Rate verwechselt werden, die genauen bounce/complaint Ereignissen entspricht, wie sie in Echtzeit auftreten, wie sie auf der Konto-Dashboard-Seite angezeigt werden).

Einfaches Beispiel zum Vergleichen der Unzustellbarkeits- oder Beschwerderaten zwischen der Seite Reputation metrics (Zuverlässigkeitsmetriken) und der Seite Account dashboard (Konto-Dashboard: Angenommen, gestern betrug die Rate 2 % und heute beträgt sie 1 %. Auf der Seite Reputation metrics (Zuverlässigkeitsmetriken) sehen Sie nur die aktuelle Rate von 1 %, die Diagramme auf der Seite Account dashboard (Konto-Dashboard) bilden jedoch den Verlauf ab, d. h. eine Rate von 2 % für gestern und 1 % für heute.

Konto-Dashboard

Sie können die Anzahl der E-Mails, die von Ihrem Konto zugestellt wurden, sowie den Prozentsatz Ihrer Sendequote, die verwendet wurde, direkt über die Seite Account dashboard (Konto-Dashboard) der SES-Konsole im Bereich Daily email usage (Tägliche E-Mail-Nutzung) überwachen. Die Zustellungs- und Ablehnungsraten für Ihr Konto können Sie im Bereich Sending

Statistics(Sendestatistiken) sowie andere wichtige Faktoren im Zusammenhang mit dem Senden von E-Mails in den folgenden Bereichen überwachen:

- Sending limits (Sendelimits) – enthält die folgenden für den E-Mail-Versand über SES geltenden Kontingente:
  - Daily sending quota (Tägliche Sendequote) – die maximale Anzahl an E-Mails, die Sie in 24 Stunden senden können
  - Maximum send rate (Maximale Senderate) – die maximale Anzahl an E-Mails, die pro Sekunde von Ihrem Konto gesendet werden können
- Account health (Kontozustand) – der Zustand Ihres SES-Kontos:
  - `Healthy` – Es gibt keine Probleme im Hinblick auf die Zuverlässigkeit, die sich derzeit auf Ihr Konto auswirken.
  - `Under review` – Es wurden potenzielle Probleme mit Ihrem SES-Konto identifiziert. – Ihr Konto wird überprüft, während Sie an der Problembehebung arbeiten.
  - `Paused` – Die Fähigkeit Ihres Kontos, E-Mails zu senden, ist derzeit aufgrund eines Problems mit der von Ihrem Konto gesendeten E-Mail unterbrochen. Wenn das Problem behoben wurde, können Sie die Wiederherstellung der Fähigkeit Ihres Kontos, E-Mails zu senden, beantragen.
- Daily email usage (Tägliche E-Mail-Nutzung) – zur Überprüfung Ihrer täglichen Nutzung, um sicherzustellen, dass Sie sich Ihren Sendelimits nicht nähern:
  - Emails sent (Gesendete E-Mails) – Gesamtzahl der in einem Zeitraum von 24 Stunden gesendeten E-Mails
  - Verbleibende Sendungen – Gesamtzahl der verbleibenden E-Mails, die Sie in einem Zeitraum von 24 Stunden senden können.
  - Verwendete Sendequote – Prozentsatz Ihrer genutzten täglichen Sendequote
- Sending statistics (Sendestatistiken) – besteht aus Diagrammen, die das Fortschreiten von vier wesentlichen Metriken in einem chronologisch sortierten Satz von Datenpunkten zeigen, die die Werte eines überwachten Ereignistyps darstellen, der Statistiken für den ausgewählten Datumsbereich mit einem Aggregationszeitraum von 1 Stunde produziert. Sie können einen Datenbereich mit Startwerten von `Last 1 day` bis `Last 14 days` auswählen, um die folgenden Diagramme zu filtern:
  - Sends (Sendevorgänge) – die Summe erfolgreicher E-Mail-Sendungsanfragen für den ausgewählten Datumsbereich
  - Rejects (Ablehnungen) – Durchschnittsrate der abgelehnten Sendungsanfragen von SES basierend auf `Rejects/Sends * 100` für den ausgewählten Datumsbereich

- Bounces (Unzustellbarkeiten) – Durchschnittsrate, die sich aus Ihren gesamten historischen Zuverlässigkeitsmetriken für den Absender ergibt, die den Fortschritt für den ausgewählten Datumsbereich anzeigen
- Complaints (Beschwerden) – Durchschnittsrate, die sich aus Ihren gesamten historischen Zuverlässigkeitsmetriken für den Absender ergibt, die den Fortschritt für den ausgewählten Datumsbereich anzeigen

Jedes dieser Diagramme enthält eine CloudWatch Schaltfläche „Anzeigen in“, mit der die jeweilige Metrik in der CloudWatch Amazon-Konsole geöffnet wird, sodass detaillierte Daten angezeigt, benutzerdefinierte Metrikberechnungen durchgeführt und Alarme erstellt werden können CloudWatch.

Zuverlässigkeitsmetriken

Zusätzlich zu den erläuterten Unzustellbarkeits- und Beschwerderaten bietet die Seite Reputation metrics (Zuverlässigkeitsmetriken) auch weitere allgemeine Einblicke in Schlüsselfaktoren, die sich auf Ihre Zuverlässigkeit auswirken, in folgenden Bereichen:

- Summary (Übersicht) – stellt einen Überblick über den Zustand Ihrer Reputation bereit
  - Status – allgemeiner Zustand der Zuverlässigkeit basierend auf historischen Unzustellbarkeits- und Beschwerderaten:
    - `Healthy` – Beide Metriken liegen innerhalb des normalen Niveaus.
    - `Under review` – Eine oder beide Metriken haben automatisch zu einer Überprüfung Ihres Kontos geführt.
    - `At risk` – Eine oder beide Metriken haben ein anormales Niveau erreicht und die Fähigkeit Ihres Kontos, E-Mails zu senden, ist möglicherweise gefährdet.
  - Gesendete E-Mails (letzte 24 Stunden) – die Gesamtzahl der im Zeitraum der letzten 24 Stunden gesendeten E-Mails.
  - Verbleibende Sendungen – Gesamtzahl der verbleibenden E-Mails, die Sie in einem Zeitraum von 24 Stunden senden können.
  - Verwendete Sendequote – Prozentsatz Ihrer genutzten täglichen Sendequote.
- Inhalt der Registerkarte „Account-level“ (Kontoebene):
  - Bounce rate (Unzustellbarkeitsrate)
    - Status – zeigt den Zustand Ihrer Unzustellbarkeitsrate unter Verwendung der gleichen Werte wie für den Bereich „Summary“ (Übersicht) beschrieben an

    - Historic bounce rate (Historische Unzustellbarkeitsrate) – Prozentsatz der E-Mails von Ihrem Konto, die eine permanente Unzustellbarkeit zur Folge hatten. Dieser Prozentsatz wird aus Ihrem historischen Gesamtdurchschnitt berechnet, basierend auf einem repräsentativen Volumen, das Ihr typisches Sendeverhalten darstellt.
  - Complaint rate (Beschwerderate)
    - Status – zeigt den Zustand Ihrer Beschwerderate unter Verwendung der gleichen Werte wie für den Bereich „Summary“ (Übersicht) beschrieben an
    - Historic bounce rate (Historische Unzustellbarkeitsrate) – Prozentsatz der von Ihrem Konto gesendeten E-Mails, die von Empfängern als Spam gemeldet wurden. Dieser Prozentsatz wird aus Ihrem historischen Gesamtdurchschnitt berechnet, basierend auf einem repräsentativen Volumen, das Ihr typisches Sendeverhalten darstellt.
- Inhalt der Registerkarte „Configuration set“ (Konfigurationssatz):
  - „Reputation by configuration set“ (Reputation nach Konfigurationssatz)
    - Configuration set (Konfigurationssatz) – ermöglicht die Eingabe oder Auswahl eines Konfigurationssatzes mit aktivierten Zuverlässigkeitsmetriken, sodass Sie Daten zur Übersicht, zur Unzustellbarkeit und zu Beschwerden basierend auf den E-Mails anzeigen können, die mit dem ausgewählten Konfigurationssatz gesendet wurden. Die Bereiche, die nach Auswahl eines Konfigurationssatzes angezeigt werden, entsprechen den oben für die Seite zu Reputationsmetriken beschriebenen Bereichen. Allerdings basieren sie nur auf E-Mails, die mit dem ausgewählten Konfigurationssatz anstatt den gesamten Sendemetriken auf Kontoebene gesendet wurden.

SMTP-Einstellungen

Auf dieser Seite sind die SMTP-Einstellungen aufgeführt, die für die Verwendung der SMTP-Schnittstelle von Amazon SES entweder über die SES-API oder programmgesteuert erforderlich sind. Die Seite enthält außerdem Links zum Erstellen und Verwalten Ihrer SMTP-Anmeldeinformationen:

- SMTP settings (SMTP-Einstellungen) – Wenn Sie eine SMTP-fähige Programmiersprache, einen E-Mail-Server oder eine Anwendung verwenden möchten, um eine Verbindung zur Amazon-SES-SMTP-Schnittstelle herzustellen, finden Sie hier die folgenden Informationen:
  - SMTP-Endpunkt
  - STARTTLS-Port
  - Transport Layer Security (TLS)

- TLS-Wrapper-Port
- Authentifizierungslinks zum Erstellen und Verwalten von SMTP- und IAM-Anmeldeinformationen

Verwenden der Konsole zum Überwachen von Sende- und Zuverlässigkeitsmetriken

Mit den folgenden Verfahren können Sie mit der Untersuchung Ihrer Sende- und Zuverlässigkeitsmetriken beginnen – entweder über die Seite Account dashboard (Konto-Dashboard) für Metriken, die auf dem aktuellen Verlauf (bis zu 14 Tage) basieren, oder über die Seite Reputation metrics (Zuverlässigkeitsmetriken) für Metriken, die auf dem Gesamtverlauf bis zum aktuellen Zeitpunkt basieren.

So zeigen Sie gesendete und verwendete Sendequote an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard) aus. Ihre Nutzungsstatistiken werden im Abschnitt Daily email usage (Tägliche E-Mail-Nutzung) angezeigt.

So zeigen Sie die Anzahl der Sendungen, Ablehnungsraten, Unzustellbarkeiten und Beschwerden an

1. Wählen Sie im Navigationsbereich Dashboard (Dashboard) aus.
2. Verwenden Sie im Abschnitt Senden von Statistiken das Dropdown Datumsbereich, um einen Startwert für einen Datumsbereich auszuwählen, um die vier Diagramme direkt unter dem Abschnitt Senden von Statistiken zu filtern.
3. Basierend auf dem ausgewählten Datumsbereich können Sie sehen, wie hoch die Zählungen und Raten in der Vergangenheit waren, die den metrischen Fortschritt der Änderungen bis zur gegenwärtigen Zeit zeigen.
4. Wählen Sie in einem der Diagramme die CloudWatch Schaltfläche „Anzeigen in“, um die entsprechende Metrik in der CloudWatchAmazon-Konsole zu öffnen, in der Sie detaillierte Daten anzeigen, benutzerdefinierte Metrikberechnungen durchführen und Überwachungsalarme erstellen können CloudWatch.

So zeigen Sie die historischen Unzustellbarkeits- und Beschwerderaten an

1. Wählen Sie im Navigationsbereich Reputation metrics (Reputationsmetriken) aus.
2. Im Bereich Bounce rate (Unzustellbarkeitsrate) können Sie den Prozentsatz der von Ihrem Konto gesendeten E-Mails anzeigen, die eine permanente Unzustellbarkeit zur Folge hatten. Im Bereich Complaint rate (Beschwerderate) können Sie den Prozentsatz der von Ihrem Konto gesendeten E-Mails anzeigen, die von Empfängern als Spam gemeldet wurden. Beide Metriken werden aus einem repräsentativen E-Mail-Volumen basierend auf Ihrem typischen Sendeverhalten berechnet.
3. Wählen Sie in einem der Bereiche die CloudWatch Schaltfläche Anzeigen in, um die entsprechende Metrik in der CloudWatchAmazon-Konsole zu öffnen, in der Sie detaillierte Daten anzeigen, benutzerdefinierte Metrikberechnungen durchführen und Überwachungsalarme erstellen können. CloudWatch

So zeigen Sie Reputationsmetriken nach Konfigurationssätzen an

1. Wählen Sie im Navigationsbereich Reputation metrics (Reputationsmetriken) aus.
2. Wählen Sie auf der Seite zu Reputationsmetriken die Registerkarte Configuration set (Konfigurationssatz) aus.
3. Klicken Sie im Bereich Reputation by configuration set (Reputation nach Konfigurationssatz) in das Feld Configuration set (Konfigurationssatz) und beginnen Sie mit der Eingabe eines Konfigurationssatzes, bei dem Reputationsmetriken aktiviert sind, oder wählen Sie einen solchen Konfigurationssatz aus.
4. Nach Auswahl des Konfigurationssatzes werden die Bereiche „Summary“ (Übersicht), „Bounce“ (Unzustellbarkeit) and „Complaint“ (Beschwerde) geladen. In diesen Bereichen werden Metriken angezeigt, die ausschließlich auf mit dem ausgewählten Konfigurationssatz gesendeten E-Mails basieren.

Überwachen der Nutzungsstatistiken mit der API von Amazon SES

Die API von Amazon SES umfasst die Operation `GetSendStatistics`, von der Informationen über Ihre Servicenutzung zurückgegeben werden. Am besten überprüfen Sie regelmäßig Ihre Sendestatistiken, damit Sie ggf. Anpassungen vornehmen können.

Bei Aufruf der API-Operation `GetSendStatistics` erhalten Sie eine Liste mit Datenpunkten, die Ihre Sendeaktivität der letzten beiden Wochen darstellen. Jeder Datenpunkt in dieser Liste stellt 15 Minuten Aktivität dar und enthält folgende Informationen für diesen Zeitraum:

- Anzahl permanenter Unzustellbarkeiten
- Anzahl der Beschwerden
- Anzahl der Zustellungsversuche (entspricht der Anzahl gesendeter E-Mails)
- Anzahl der abgelehnten Sendeversuche
- Zeitstempel für den Analysezeitraum

Eine vollständige Beschreibung der `GetSendStatistics`-Operation finden Sie im Abschnitt Amazon Simple Email Service API-Referenz.

In diesem Abschnitt werden die folgenden Themen behandelt:

- the section called “Aufrufen der `GetSendStatistics` API-Operation mit dem AWS CLI”
- the section called “Programmgesteuertes Aufrufen der Operation `GetSendStatistics`”

Aufrufen der **`GetSendStatistics`** API-Operation mit dem AWS CLI

Die einfachste Methode zum Aufrufen der API-Operation `GetSendStatistics` bietet die AWS Command Line Interface (AWS CLI).

Um den **`GetSendStatistics`** API-Vorgang mit dem aufzurufen AWS CLI

1. Sofern noch nicht geschehen, installieren Sie die AWS CLI. Weitere Informationen finden Sie unter "Installation von AWS Command Line Interface" im AWS Command Line Interface Benutzerhandbuch.
2. Falls Sie dies noch nicht getan haben, konfigurieren Sie den AWS CLI so, dass er Ihre AWS Anmeldeinformationen verwendet. Weitere Informationen finden Sie unter "Konfiguration von AWS CLI" im AWS Command Line Interface Benutzerhandbuch.
3. Führen Sie in der Befehlszeile den folgenden Befehl aus.

```
aws ses get-send-statistics
```

Wenn der richtig konfiguriert AWS CLI ist, wird eine Liste mit Sendestatistiken im JSON-Format angezeigt. Jedes JSON-Objekt enthält die zusammengefassten Sendestatistiken für einen Zeitraum von 15 Minuten.

Programmgesteuertes Aufrufen der Operation **`GetSendStatistics`**

Sie können den `GetSendStatistics` Vorgang auch mit dem aufrufen AWS SDKs. Dieser Abschnitt enthält Codebeispiele AWS SDKs für Go, PHP, Python und Ruby. Klicken Sie auf einen der folgenden Links, um das Codebeispiel für die jeweilige Sprache aufzurufen:

- Codebeispiel für das AWS SDK für Go
- Codebeispiel für das AWS SDK für PHP
- Codebeispiel für das AWS SDK für Python (Boto)
- Codebeispiel für das AWS SDK für Ruby

> **Note**
>
> Bei diesen Codebeispielen wird davon ausgegangen, dass Sie eine Datei mit AWS gemeinsamen Anmeldeinformationen erstellt haben, die Ihre AWS Zugriffsschlüssel-ID, Ihren AWS geheimen Zugriffsschlüssel und Ihre bevorzugte AWS Region enthält. Weitere Informationen finden Sie unter Konfigurations- und Anmeldeinformationsdateien.

Rufen **`GetSendStatistics`** Sie mit dem AWS SDK für Go

```
package main

import (
    "fmt"

    //go get github.com/aws/aws-sdk-go/...
    "github.com/aws/aws-sdk-go/aws"
    "github.com/aws/aws-sdk-go/aws/session"
    "github.com/aws/aws-sdk-go/service/ses"
    "github.com/aws/aws-sdk-go/aws/awserr"
)
```

```
const (
    // Replace us-west-2 with the AWS Region you're using for Amazon SES.
    AwsRegion = "us-west-2"
)

func main() {

    // Create a new session and specify an AWS Region.
    sess, err := session.NewSession(&aws.Config{
        Region:aws.String(AwsRegion)},
    )

    // Create an SES client in the session.
    svc := ses.New(sess)
    input := &ses.GetSendStatisticsInput{}

    result, err := svc.GetSendStatistics(input)

    // Display error messages if they occur.
    if err != nil {
        if aerr, ok := err.(awserr.Error); ok {
            switch aerr.Code() {
            default:
                fmt.Println(aerr.Error())
            }
        } else {
            // Print the error, cast err to awserr.Error to get the Code and
            // Message from an error.
            fmt.Println(err.Error())
        }
        return
    }

    fmt.Println(result)
}
```

Anrufen **`GetSendStatistics`** mit dem AWS SDK für PHP

```
<?php

// Replace path_to_sdk_inclusion with the path to the SDK as described in
// http://docs.aws.amazon.com/aws-sdk-php/v3/guide/getting-started/basic-usage.html
define('REQUIRED_FILE','path_to_sdk_inclusion');
```

```
// Replace us-west-2 with the AWS Region you're using for Amazon SES.
define('REGION','us-west-2');

require REQUIRED_FILE;

use Aws\Ses\SesClient;

$client = SesClient::factory(array(
    'version'=> 'latest',
    'region' => REGION
));

try {
     $result = $client->getSendStatistics([]);
  echo($result);
} catch (Exception $e) {
     echo($e->getMessage()."\n");
}

?>
```

Anrufen **`GetSendStatistics`** mit dem AWS SDK für Python (Boto)

```
import boto3 #pip install boto3
import json
from botocore.exceptions import ClientError

client = boto3.client('ses')

try:
    response = client.get_send_statistics(
)
except ClientError as e:
    print(e.response['Error']['Message'])
else:
    print(json.dumps(response, indent=4, sort_keys=True, default=str))
```

Anrufen **`GetSendStatistics`** mit dem AWS SDK für Ruby

```
require 'aws-sdk' # gem install aws-sdk
require 'json'
```

```
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
awsregion = "us-west-2"

# Create a new SES resource and specify a region
ses = Aws::SES::Client.new(region: awsregion)

begin

  resp = ses.get_send_statistics({
  })
  puts JSON.pretty_generate(resp.to_h)

# If something goes wrong, display an error message.
rescue Aws::SES::Errors::ServiceError => error
  puts error

end
```

Überwachen des E-Mail-Versands mithilfe der Amazon SES-Ereignisveröffentlichung

Damit Sie Ihren E-Mail-Versand detailliert verfolgen können, können Sie Amazon SES so einrichten, dass E-Mail-Versandereignisse auf EventBridge Grundlage von von Ihnen definierten Merkmalen an Amazon CloudWatch, Amazon Data Firehose, Amazon Pinpoint, Amazon Simple Notification Service oder Amazon veröffentlicht werden.

Sie können mehrere Arten von E-Mail-Sendeereignissen nachverfolgen, einschließlich gesendete, zugestellte, geöffnete, angeklickte, unzustellbare und abgelehnte E-Mails sowie Beschwerden, Rendering-Fehler und Zustellverzögerungen. Diese Informationen helfen Ihnen bei betrieblichen und analytischen Zwecken. Sie können beispielsweise Ihre E-Mail-Versanddaten veröffentlichen CloudWatch und Dashboards erstellen, die die Leistung Ihrer E-Mail-Kampagnen verfolgen, oder Sie können Amazon SNS verwenden, um Ihnen Benachrichtigungen zu senden, wenn bestimmte Ereignisse eintreten.

So funktioniert die Veröffentlichung von Ereignissen mit Konfigurationssätzen und Nachrichten-Tags

Zur Verwendung der Ereignisveröffentlichung müssen Sie zunächst ein oder mehrere Konfigurationssätze einrichten. Ein Konfigurationssatz gibt an, wo Ihre Ereignisse veröffentlicht werden und welche Ereignisse veröffentlicht werden. Anschließend geben Sie jedes Mal, wenn Sie eine E-Mail senden, den Namen des Konfigurationssatzes und ein oder mehrere Nachrichten-Tags in Form von name/value Paaren an, um die E-Mail zu kategorisieren. Wenn Sie beispielsweise Bücher bewerben, könnten Sie einen Nachrichten-Tag Genre nennen und den Wert Sci-Fi oder Western zuweisen, wenn Sie eine E-Mail für die entsprechende Kampagne senden.

Je nachdem, welche E-Mail-Versandschnittstelle Sie verwenden, geben Sie entweder das Nachrichten-Tag als Parameter für das `EmailTags`Feld der `SendEmail`API-Operation an oder fügen das Nachrichten-Tag dem SES-spezifischen E-Mail-Header hinzu. `X-SES-MESSAGE-TAGS` Weitere Informationen zu Konfigurationssätzen finden Sie unter Verwenden von Amazon SES-Konfigurationssätzen im.

Zusätzlich zu den von Ihnen angegebenen Nachrichten-Tags fügt SES den von Ihnen gesendeten Nachrichten auch Auto-Tags hinzu. Sie müssen keine weiteren Schritte zum Verwenden der automatischen Tags durchführen.

In der folgenden Tabelle sind die Auto-Tags aufgeführt, die automatisch auf Nachrichten angewendet werden, die Sie mit SES senden.

SES-Auto-Tags

Automatische Tag-Namen	Description
`ses:caller-identity`	Die IAM-Identität des SES-Benutzers, der die E-Mail gesendet hat.
`ses:configuration-set`	Der Name des Konfigurationssatzes, der der E-Mail zugeordnet ist.
`ses:from-domain`	Die Domäne der "From"-Adresse.
`ses:outgoing-ip`	Die IP-Adresse, die SES zum Senden der E-Mail verwendet hat.

Automatische Tag-Namen	Description
`ses:source-ip`	Die IP-Adresse, die der Aufrufer zum Senden der E-Mail verwendet hat.
`ses:source-tls-version`	Die TLS-Protokollversion, mit der der Anrufer die E-Mail gesendet hat.
`ses:outgoing-tls-version`	Die TLS-Protokollversion, die SES zum Senden der E-Mail verwendet hat.

Detailliertes Feedback für E-Mail-Kampagnen

Das `ses:feedback-id-<a or b>` Tag ist ein optionales Nachrichten-Tag, das Sie sich als hybrides oder halbautomatisches Tag vorstellen können. Es ähnelt zwar den im vorherigen Abschnitt besprochenen Auto-Tags, der Unterschied besteht jedoch darin, dass Sie es manuell hinzufügen und den Präfixschlüssel verwenden müssen. `ses:` Sie können bis zu zwei dieser Tags verwenden, die als und definiert sind. `ses:feedback-id-a` `ses:feedback-id-b`

Wenn Sie diese Tags angeben, hängt SES sie automatisch an den `Feedback-ID` Standard-Header an, der für die Bereitstellung von Zustellungsstatistiken wie Beschwerden und Spamraten als Teil einer Feedback-Schleife (FBL) verwendet wird, siehe. Feedback-Schleifen Der `Feedback-ID` Header besteht aus der Kennung (SESInternalID), die von SES für die Erfassung von Beschwerdeinformationen verwendet wird, und dem statischen Tag AmazonSES, das SES als Versandplattform identifiziert, z. B.:

```
FeedBackId:feedback-id-a:feedback-id-b:((SESInternalID):(AmazonSES))
```

Diese optionalen Feedback-ID-Tags bieten Ihnen die Möglichkeit, detailliertes Feedback zu generieren, z. B. für Nachrichten, die Sie im Rahmen einer E-Mail-Kampagne versenden. Sie können es verwenden, `ses:feedback-id-<a or b>` indem Sie es als Nachrichten-Tag im `EmailTags`Feld der `SendEmail`Operationsanfrage angeben, wie im folgenden Beispiel gezeigt:

```
{
  "FromEmailAddress": "noreply@example.com",
  "Destination": {
    "ToAddresses": [
      "customer@example.net"
    ]
```

```
  },
  "Content": {
    "Simple": {
      "Subject": {
        "Data": "Hello and welcome"
      },
      "Body": {
        "Text": {
          "Data": "Lorem ipsum dolor sit amet."
        },
        "Html": {
          "Data": "Lorem ipsum dolor sit amet."
        }
      }
    }
  },
  "EmailTags": [
    {
      "Name": "ses:feedback-id-a",
      "Value": "new-members-campaign"
    },
    {
      "Name": "ses:feedback-id-b",
      "Value": "football-campaign"
    }
  ],
  "ConfigurationSetName": "football-club"
}
```

Wenn Sie im Rohformat senden, würden Sie dem SES-spezifischen Header ein Nachrichten-Tag hinzufügen`ses:feedback-id-<a or b>`. X-SES-MESSAGE-TAGS

Das `ses:feedback-id-<a or b>` Nachrichten-Tag kann auch in Amazon nachverfolgt werden, CloudWatch indem es wie jedes andere Nachrichten-Tag als CloudWatch Wertquelle angegeben wird, siehe the section called “Details zum Ziel des CloudWatch Ereignisses hinzufügen” (Es fallen zusätzliche Gebühren an, siehe Preis pro Metrik für CloudWatch.)

Verwenden der Ereignisveröffentlichung

Die folgenden Abschnitte enthalten die Informationen, die Sie für die Einrichtung und Nutzung von SES Event Publishing benötigen.

- Einrichten der Ereignisveröffentlichung

- Arbeiten mit Ereignisdaten

Terminologie zu Ereignisveröffentlichung

In der folgenden Liste werden Begriffe im Zusammenhang mit der Veröffentlichung von SES-Veranstaltungen definiert.

E-Mail-Sendeereignis

Informationen im Zusammenhang mit dem Ergebnis einer E-Mail, die Sie an SES senden. Das Senden von Ereignissen umfasst Folgendes:

- Send (Senden) – die Sendeanfrage war erfolgreich und Amazon SES versucht, dem E-Mail-Server des Empfängers die Nachricht zuzustellen. (Wenn eine Unterdrückung auf Kontoebene oder eine globale Unterdrückung verwendet wird, zählt SES sie weiterhin als Senden, aber die Zustellung wird unterdrückt.)
- RenderingFailure— Die E-Mail wurde aufgrund eines Problems beim Rendern der Vorlage nicht gesendet. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail-Vorlage mithilfe der `SendTemplatedEmail`- oder `SendBulkTemplatedEmail`-API-Operationen senden.
- Rejects (Ablehnungen) – Amazon SES hat die E-Mail akzeptiert, aber festgestellt, dass sie einen Virus enthielt und nicht versucht hat, ihn an den Mail-Server des Empfängers zu übermitteln.
- Delivery (Zustellung) – Amazon SES hat die E-Mail erfolgreich an den Mail-Server des Empfängers übermittelt.
- Bounce – eine permanente Unzustellbarkeit, sodass die E-Mail vom E-Mail-Server des Empfängers dauerhaft abgelehnt wurde. (Soft Bounces sind nur enthalten, wenn SES nicht mehr versucht, die E-Mail zuzustellen. Im Allgemeinen deuten diese Soft Bounces auf einen Zustellungsfehler hin, obwohl in einigen Fällen ein Soft Bounce auch dann zurückgegeben werden kann, wenn die E-Mail den Posteingang des Empfängers erfolgreich erreicht hat. Dies tritt normalerweise auf, wenn der Empfänger eine out-of-office automatische Antwort sendet. In diesem AWS re:POST-Artikel erfährst du mehr über Soft Bounces.)
- Complaint (Beschwerde) – die E-Mail wurde erfolgreich an den E-Mail-Server des Empfängers gesendet, der Empfänger hat sie jedoch als Spam markiert.
- DeliveryDelay— Die E-Mail konnte nicht an den Mailserver des Empfängers zugestellt werden, da ein vorübergehendes Problem aufgetreten ist. Verzögerungen bei der Zustellung können,

z. B. auftreten, wenn der Posteingang des Empfängers voll ist oder der empfangende E-Mail-Server ein vorübergehendes Problem aufweist.

- Subscription (Abonnement) – die E-Mail wurde erfolgreich zugestellt, aber der Empfänger hat die Abonnementeinstellungen aktualisiert, indem er auf `List-Unsubscribe` in der E-Mail-Kopfzeile oder auf den `Unsubscribe`-Link in der Fußzeile geklickt hat.
- Open (Geöffnet) – der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
- Click (Klick) – der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.

Konfigurationssatz

Eine Reihe von Regeln, die das Ziel definieren, an das SES E-Mail-Versandereignisse veröffentlicht, und die Arten von E-Mail-Versandereignissen, die Sie veröffentlichen möchten. Wenn Sie eine E-Mail senden, die Sie mit der Ereignisveröffentlichung verwenden möchten, geben Sie den Konfigurationssatz an, der der E-Mail zugeordnet werden soll.

Ereignisziel

Ein AWS Dienst, für den Sie SES-E-Mail-Versandereignisse veröffentlichen. Jedes eingerichtete Ereignisziel gehört zu einem einzigen Konfigurationssatz.

Nachrichten-Tag

Ein name/value Paar, das Sie verwenden, um eine E-Mail für die Veröffentlichung von Ereignissen zu kategorisieren. Beispiele sind Kampagne/Buch und Kampagne/Bekleidung. Wenn Sie eine E-Mail senden, geben Sie das Nachrichten-Tag entweder als Parameter für den API-Aufruf oder als SES-spezifischen E-Mail-Header an.

Automatisches Tag

Nachrichten-Tags, die automatisch in Berichten zur Ereignisveröffentlichung enthalten sind. Es gibt ein Auto-Tag für den Namen des Konfigurationssatzes, die Domäne der Absenderadresse, die ausgehende IP-Adresse des Anrufers, die ausgehende SES-IP-Adresse und die IAM-Identität des Anrufers.

Einrichten der Amazon SES-Ereignisveröffentlichung

In diesem Abschnitt wird beschrieben, was Sie tun müssen, um Amazon SES so zu konfigurieren, dass Ihre E-Mail-Versandereignisse für die folgenden AWS Dienste veröffentlicht werden:

- Amazon CloudWatch

- Amazon Data Firehose
- Amazon Pinpoint
- Amazon-Simple-Notification-Service (Amazon-SNS)

Die folgenden Schritte, die zum Einrichten der Ereignisveröffentlichung erforderlich sind, werden in den folgenden Themen behandelt:

1. Zuerst erstellen Sie einen Konfigurationssatz mit der Amazon SES-Konsole oder der API.
2. Fügen Sie dem Konfigurationssatz ein oder mehrere Ereignisziele (CloudWatchFirehose, Pinpoint oder SNS) hinzu und konfigurieren Sie eindeutige Parameter für das Ereignisziel.
3. Geben Sie einen Konfigurationssatz an, der das Ereignisziel beim Senden von E-Mails mit verwendet.

Themen in diesem Abschnitt

- Schritt 1: Erstellen eines Konfigurationssatzes
- Schritt 2: Hinzufügen eines Ereignisziels
- Schritt 3: Festlegen eines Konfigurationssatzes für das Senden von E-Mail

Schritt 1: Erstellen eines Konfigurationssatzes

Sie müssen zunächst über eine Konfiguration verfügen, um die Ereignisveröffentlichung einzurichten. Wenn Sie noch keinen Konfigurationssatz haben oder eine neue erstellen möchten, lesen Sie bitteVerwalten der SES Konfigurationssätze

Sie können Konfigurationssätze auch mithilfe der CreateConfigurationSetOperation in der Amazon SES API V2 oder der Amazon SES CLI v2 erstellen, sieheKonfigurationssatz erstellen (AWS CLI).

Schritt 2: Hinzufügen eines Ereignisziels

Ereignisziele sind Orte, an denen Sie Amazon SES-Ereignisse veröffentlichen. Jedes eingerichtete Ereignisziel gehört zu einem einzigen Konfigurationssatz. Wenn Sie ein Ereignisziel mit Amazon SES einrichten, wählen Sie das AWS Serviceziel aus und geben die mit diesem Ziel verknüpften Parameter an.

Wenn Sie ein Veranstaltungsziel einrichten, können Sie wählen, ob Ereignisse an einen der folgenden AWS Dienste gesendet werden sollen:

- Amazon CloudWatch
- Amazon Data Firehose
- Amazon EventBridge
- Amazon Pinpoint
- Amazon-Simple-Notification-Service (Amazon-SNS)

Welches Ereignisziel Sie auswählen, hängt davon ab, wie detailliert die Ereignisse sein sollen und auf welche Art und Weise Sie die Ereignisinformationen erhalten möchten. Möchten Sie einfach eine laufende Gesamtanzahl der einzelnen Ereignistypen erhalten (sodass Sie beispielsweise einen Alarm bei einer zu hohen Gesamtanzahl festlegen können), verwenden Sie CloudWatch.

Wenn Sie detaillierte Ereignisaufzeichnungen wünschen, die Sie zur Analyse an einen anderen Service wie Amazon OpenSearch Service oder Amazon Redshift ausgeben können, können Sie Firehose verwenden.

Falls Sie Benachrichtigungen erhalten möchten, wenn bestimmte Ereignisse eintreten, verwenden Sie Amazon SNS.

In diesem Abschnitt werden folgende Themen beschrieben

- Richten Sie ein CloudWatch Veranstaltungsziel für die Veröffentlichung von Veranstaltungen ein
- Richten Sie ein Data Firehose-Ereignisziel für die Veröffentlichung von Amazon SES SES-Ereignissen ein
- Richten Sie ein EventBridge Amazon-Ziel für die Veröffentlichung von Veranstaltungen ein
- Einrichten eines Amazon-Pinpoint-Ereignisziels für die Ereignisveröffentlichung
- Einrichten eines Amazon SNS-Ereignisziels für die Ereignisveröffentlichung

Richten Sie ein CloudWatch Veranstaltungsziel für die Veröffentlichung von Veranstaltungen ein

Mit Amazon CloudWatch Metrics können Sie Ereignisziele verwenden, um Amazon SES E-Mail-Versandereignisse zu veröffentlichen CloudWatch. Da ein CloudWatch Ereignisziel nur in einem Konfigurationssatz eingerichtet werden kann, müssen Sie zuerst einen Konfigurationssatz erstellen und dann das Ereignisziel dem Konfigurationssatz hinzufügen.

Wenn Sie einem Konfigurationssatz ein CloudWatch Ereignisziel hinzufügen, müssen Sie eine oder mehrere CloudWatch Dimensionen auswählen, die den Nachrichten-Tags entsprechen, die Sie beim

Senden Ihrer E-Mails verwenden. Wie Nachrichten-Tags ist eine CloudWatch Dimension ein name/value Paar, das Ihnen hilft, eine Metrik eindeutig zu identifizieren.

Sie können beispielsweise ein Nachrichten-Tag und eine Dimension mit dem Namen `campaign` verwenden, um Ihre E-Mail-Kampagne zu identifizieren. Wenn Sie Ihre E-Mail-Versandereignisse für veröffentlichen CloudWatch, ist es wichtig, Ihre Nachrichten-Tags und Dimensionen auszuwählen, da sich diese Optionen auf Ihre CloudWatch Abrechnung auswirken und bestimmen, wie Sie Ihre E-Mail-Versandereignisdaten filtern können CloudWatch.

Dieser Abschnitt enthält Informationen, die Ihnen bei der Auswahl Ihrer Dimensionen helfen, und zeigt anschließend, wie Sie einem Konfigurationssatz ein CloudWatch Veranstaltungsziel hinzufügen.

Themen in diesem Abschnitt

- Hinzufügen eines CloudWatch Veranstaltungsziels
- CloudWatch Dimensionen auswählen

Hinzufügen eines CloudWatch Veranstaltungsziels

Das Verfahren in diesem Abschnitt zeigt, wie Sie Details zum Ziel eines CloudWatch Ereignisses zu einem Konfigurationssatz hinzufügen. Dabei wird vorausgesetzt, dass Sie die Schritte 1 bis 6 unter abgeschlossen habenErstellen eines Ereignisziels.

Sie können den UpdateConfigurationSetEventDestinationVorgang auch in der Amazon SES API V2 verwenden, um Ereignisziele zu erstellen und zu ändern.

So fügen Sie mithilfe der Konsole Details zum Ziel eines CloudWatch Ereignisses zu einem Konfigurationssatz hinzu

1. Dies sind die detaillierten Anweisungen zur Auswahl CloudWatch des Zieltyps für Ihr Ereignis in Schritt 7, wobei davon ausgegangen wird, dass Sie alle vorherigen Schritte unter abgeschlossen habenErstellen eines Ereignisziels. Nachdem Sie den CloudWatch Zieltyp ausgewählt, einen Zielnamen eingegeben und die Veröffentlichung von Ereignissen aktiviert haben, wird der Bereich CloudWatch Amazon-Dimensionen angezeigt. Die entsprechenden Felder werden in den folgenden Schritten behandelt. (Es fallen zusätzliche Gebühren an, siehe Preis pro Metrik für.) CloudWatch
2. Geben Sie für Value Source an, wie Amazon SES die Daten erhält, an die es weitergibt CloudWatch. Die folgenden Quellen für Werte sind verfügbar:

- Message Tag (Nachrichten-Tag) – Amazon SES ruft den Dimensionsnamen und Wert aus einem Tag ab, der von Ihnen mittels eines `X-SES-MESSAGE-TAGS`-Headers oder eines Parameters für die `EmailTags`-API angegeben wurde. Weitere Informationen zur Verwendung von Nachrichten-Tags finden Sie unter the section called “Schritt 3: Festlegen eines Konfigurationssatzes für den Versand”.

  > **Note**
  >
  > Nachrichten-Tags können die Zahlen 0-9, die Buchstaben A-Z (Groß- und Kleinbuchstaben), Bindestriche (-) und Unterstriche (_) enthalten.

  Sie können auch mithilfe der Wertquelle Message Tag (Nachrichten-Tag) Dimensionen basierend auf automatischen Amazon SES-Tags erstellen. Sie können einen automatischen Tag verwenden, indem Sie unter Dimension Name (Dimensionsname) den vollständigen Namen des automatischen Tag eingeben. Um z. B. eine Dimension basierend auf dem automatischen Tag des Konfigurationssatzes zu erstellen, verwenden Sie `ses:configuration-set` für den Dimension Name (Dimensionsname) und den Namen des Konfigurationssatzes für Default Value (Standardwert). Eine vollständige Liste automatischer Tags finden Sie unter So funktioniert die Veröffentlichung von Ereignissen mit Konfigurationssätzen und Nachrichten-Tags.

- Email Header (E-Mail-Überschrift) – Amazon SES ruft den Dimensionsnamen und Wert aus einem Header in der E-Mail ab.

  > **Note**
  >
  > Die folgenden E-Mail-Header dürfen nicht als Dimension Name (Dimensionsname) verwendet werden: `Received`, `To`, `From`, `DKIM-Signature`, `CC`, `message-id` oder `Return-Path`.

- Link Tag (Link-Tag) – Amazon SES ruft den Dimensionsnamen und den Wert aus einem Tag ab, der von Ihnen in einem Link angegeben wurde. Weitere Informationen zum Hinzufügen von Tags zu Links finden Sie unter Kann ich Links mit eindeutigen Bezeichnern markieren?.

3. Geben Sie unter Dimension Name (Dimensionsname) den Namen der Dimension ein, die Sie an CloudWatch übergeben möchten.

> **Note**
>
> Dimensionsnamen dürfen nur ASCII-Buchstaben (a-z, A-Z), Zahlen (0-9), Unterstriche (_) und Bindestriche (-) enthalten. Leerzeichen, Akzentbuchstaben, nicht-lateinische Zeichen und andere Sonderzeichen sind nicht zulässig.

4. Geben Sie unter Default Value (Standartwert) den Wert der Dimension ein.

> **Note**
>
> Dimensionswerte dürfen nur ASCII-Buchstaben (a-z, A-Z), Ziffern (0-9), Unterstriche (_), Bindestriche (-), bei Zeichen (@) und Punkte (.) enthalten. Leerzeichen, Akzentbuchstaben, nicht-lateinische Zeichen und andere Sonderzeichen sind nicht zulässig.

5. Wenn Sie weitere Dimensionen hinzufügen möchten, wählen Sie Add Dimension (Dimension hinzufügen) aus. Klicken Sie andernfalls auf Next (Weiter).
6. Wenn Sie auf dem Review-Bildschirm mit der Definition Ihres Veranstaltungsziels zufrieden sind, wählen Sie Add destination (Ziel hinzufügen) aus.

CloudWatch Dimensionen auswählen

Wenn Sie Namen und Werte als CloudWatch Dimensionen auswählen, sollten Sie die folgenden Faktoren berücksichtigen:

- Preis pro Metrik — Sie können grundlegende Amazon SES SES-Metriken CloudWatch kostenlos einsehen. Wenn Sie Metriken mithilfe von Event-Publishing erfassen, fallen jedoch Kosten für die CloudWatch detaillierte Überwachung an. Jede eindeutige Kombination aus Ereignistyp, Dimensionsname und Dimensionswert erzeugt eine andere Metrik in CloudWatch. Wenn Sie Detailed Monitoring verwenden CloudWatch, wird Ihnen jede Metrik in Rechnung gestellt. Aus diesem Grund sollten Sie vermeiden, Dimensionen auszuwählen, die viele verschiedene Werte haben können. Sie sollten z. B. keine Dimension für das automatische Amazon SES-Tag `ses:from-domain` definieren, da es viele verschiedene Werte annehmen kann, es sei denn, Sie sind sehr daran interessiert, Ihre E-Mail-Sendeereignisse nach "From" (Von)-Domäne zu verfolgen. Weitere Informationen finden Sie unter CloudWatch – Preise.

- Metrikfilterung — Wenn eine Metrik mehrere Dimensionen hat, können Sie nicht separat auf die Metrik zugreifen, die auf jeder Dimension CloudWatch basiert. Aus diesem Grund sollten Sie sorgfältig überlegen, bevor Sie einem einzelnen CloudWatch Eventziel mehr als eine Dimension hinzufügen. Wenn Sie z. B. Metriken je `campaign` und je Kombination aus `campaign` und `genre` möchten, müssen Sie zwei Ereignisziele hinzufügen: eins, das nur `campaign` als Dimension hat, und eins, das sowohl über `campaign` als auch `genre` als Dimensionen verfügt.
- Dimension value source (Dimensionswertquelle) – Sie können Dimensionswerte nicht nur mithilfe Amazon SES-spezifischer Header oder eines Parameters für die API angeben. Alternativ können Sie auch mit Amazon SES Dimensionswerte aus Ihren eigenen MIME-Nachrichten-Headern abrufen. Verwenden Sie diese Option, wenn Sie bereits benutzerdefinierte Header nutzen und Sie Ihre E-Mails oder Ihre Aufrufe an die E-Mail sendende API nicht ändern möchten, um Metriken auf der Grundlage ihrer Header-Werte zu erfassen. Wenn Sie eigene MIME-Nachrichten-Header für Amazon SES-Ereignisveröffentlichungen verwenden, dürfen die Header-Namen und Werte, die Sie für die Amazon SES-Ereignisveröffentlichung verwenden, nur die Buchstaben A bis Z, die Ziffern 0 bis 9, Unterstriche (_), at-Zeichen (@), Bindestriche (-) und Punkte (.) enthalten. Wenn Sie einen Namen oder Wert angeben, der andere Zeichen enthält, ist der E-Mail-Versandaufruf trotzdem erfolgreich, aber die Event-Metriken werden nicht an Amazon gesendet CloudWatch.

Weitere Informationen zu CloudWatch Konzepten finden Sie unter Amazon CloudWatch Concepts im CloudWatch Amazon-Benutzerhandbuch.

Richten Sie ein Data Firehose-Ereignisziel für die Veröffentlichung von Amazon SES SES-Ereignissen ein

Ein Amazon Data Firehose-Ereignisziel steht für eine Entität, die bestimmte Amazon SES SES-E-Mail-Sendeereignisse an Firehose veröffentlicht. Da ein Firehose-Ereignisziel nur in einem Konfigurationssatz eingerichtet werden kann, müssen Sie zunächst einen Konfigurationssatz erstellen. Als Nächstes fügen Sie dem Konfigurationssatz das Ereignisziel hinzu.

Das Verfahren in diesem Abschnitt zeigt, wie Sie Firehose-Ereigniszieldetails zu einem Konfigurationssatz hinzufügen, und es wird davon ausgegangen, dass Sie die Schritte 1 bis 6 unter abgeschlossen haben. Erstellen eines Ereignisziels

Sie können den UpdateConfigurationSetEventDestinationVorgang auch im Amazon SES API V2-Ziel verwenden, um Ereignisziele zu erstellen und zu aktualisieren.

So fügen Sie Firehose-Ereigniszieldetails zu einem Konfigurationssatz mithilfe der Konsole hinzu

1. Dies sind die detaillierten Anweisungen zur Auswahl von Firehose als Veranstaltungszieltyp in Schritt 7 und es wird davon ausgegangen, dass Sie alle vorherigen Schritte unter abgeschlossen haben. Erstellen eines Ereignisziels Nachdem Sie den Firehose-Zieltyp ausgewählt, einen Zielnamen eingegeben und die Veröffentlichung von Ereignissen aktiviert haben, wird der Bereich Amazon Data Firehose Delivery Stream angezeigt. Seine Felder werden in den folgenden Schritten behandelt.
2. Wählen Sie für Delivery Stream einen vorhandenen Firehose-Lieferstream aus, oder wählen Sie Neuen Stream erstellen, um mit der Firehose-Konsole einen neuen Stream zu erstellen.

   Informationen zum Erstellen eines Streams mit der Firehose-Konsole finden Sie unter Creating an Amazon Kinesis Firehose Delivery Stream im Amazon Data Firehose Developer Guide.
3. Wählen Sie für Identity and Access Management (IAM) eine IAM-Rolle aus, für die Amazon SES berechtigt ist, in Ihrem Namen auf Firehose zu veröffentlichen. Sie können eine vorhandene Rolle auswählen, Amazon SES eine Rolle für Sie erstellen lassen oder Ihre eigene Rolle erstellen.

   Wenn Sie eine bestehende Rolle wählen oder Ihre eigene Rolle erstellen, müssen Sie die Richtlinien der Rolle manuell ändern, um der Rolle die Erlaubnis zu erteilen, auf den Firehose-Lieferstream zuzugreifen, und um Amazon SES die Erlaubnis zu erteilen, die Rolle zu übernehmen. Beispiele für Richtlinien finden Sie unter Amazon SES die Erlaubnis zur Veröffentlichung in Ihrem Firehose Delivery Stream erteilen.
4. Wählen Sie Next (Weiter).
5. Wenn Sie auf dem Review-Bildschirm mit der Definition Ihres Veranstaltungsziels zufrieden sind, wählen SieHinzufügen eines Zielsaus.

Informationen zur Verwendung der `UpdateConfigurationSetEventDestination` API zum Hinzufügen eines Firehose-Ereignisziels finden Sie in der Amazon Simple Email Service API-Referenz.

Amazon SES die Erlaubnis zur Veröffentlichung in Ihrem Firehose Delivery Stream erteilen

Damit Amazon SES Datensätze in Ihrem Firehose-Lieferstream veröffentlichen kann, müssen Sie eine AWS Identity and Access Management (IAM-) Rolle verwenden und die Berechtigungsrichtlinie und Vertrauensrichtlinie der Rolle anhängen oder ändern. Die Berechtigungsrichtlinie ermöglicht es

der Rolle, Datensätze in Ihrem Firehose-Lieferstream zu veröffentlichen, und die Vertrauensrichtlinie ermöglicht es Amazon SES, die Rolle zu übernehmen.

Dieser Abschnitt enthält Beispiele für beide Richtlinien. Weitere Informationen zum Anfügen von Richtlinien an IAM-Rollen finden Sie unter Ändern einer Rolle im IAM-Benutzerhandbuch.

Berechtigungsrichtlinie

Die folgende Berechtigungsrichtlinie ermöglicht es der Rolle, Datensätze in Ihrem Firehose-Lieferstream zu veröffentlichen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Action": [
                "firehose:PutRecordBatch"
            ],
            "Resource": [
                "arn:aws:firehose:us-east-1:111122223333:deliverystream/delivery-stream-name"
            ]
        }
    ]
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- *delivery-region*Ersetzen Sie durch die AWS Region, in der Sie den Firehose-Lieferstream erstellt haben.
- Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID.
- *delivery-stream-name*Ersetzen Sie es durch den Namen des Firehose-Lieferdatenstroms.

Vertrauensrichtlinie

Die folgende Vertrauensrichtlinie ermöglicht Amazon SES die Rolle zu übernehmen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "111122223333",
          "AWS:SourceArn": "arn:aws:ses:delivery-
region:111122223333:configuration-set/configuration-set-name"
        }
      }
    }
  ]
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- *delivery-region*Ersetzen Sie durch die AWS Region, in der Sie den Firehose-Lieferstream erstellt haben.
- Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID.
- *configuration-set-name*Ersetzen Sie es durch den Namen Ihres Konfigurationssatzes, der dem Firehose-Lieferstream zugeordnet ist.

Richten Sie ein EventBridge Amazon-Ziel für die Veröffentlichung von Veranstaltungen ein

Ein EventBridge Amazon-Ereignisziel benachrichtigt Sie über die E-Mail-Versandereignisse, die Sie in einem Konfigurationssatz angeben. SES generiert und sendet E-Mail-Sendeereignisse, die Sie bei der Erstellung eines Ereignisziels definieren, an den EventBridge Standard-Event-Bus. Ein Eventbus ist ein Router, der Ereignisse empfängt und sie an mehrere Ziele weiterleiten kann. Weitere Informationen zur Integration von E-Mail-Versandereignissen mit Amazon finden Sie EventBridge

unterÜberwachung mit EventBridge. Da ein EventBridge Ereignisziel nur in einem Konfigurationssatz eingerichtet werden kann, müssen Sie einen Konfigurationssatz erstellen, bevor Sie das Ereignisziel zum Konfigurationssatz hinzufügen.

Das Verfahren in diesem Abschnitt zeigt, wie Sie einem Konfigurationssatz Details zu einem EventBridge Ereignisziel hinzufügen, und es wird davon ausgegangen, dass Sie die Schritte 1 bis 6 unter abgeschlossen habenErstellen eines Ereignisziels.

Sie können den UpdateConfigurationSetEventDestinationVorgang auch in der Amazon SES API V2 verwenden, um Ereignisziele zu erstellen und zu ändern.

So fügen Sie mithilfe der Konsole Details zum Ziel eines EventBridge Ereignisses zu einem Konfigurationssatz hinzu

1. Dies sind die detaillierten Anweisungen zur Auswahl EventBridge des Zieltyps für Ihr Ereignis in Schritt 7, wobei davon ausgegangen wird, dass Sie alle vorherigen Schritte unter abgeschlossen habenErstellen eines Ereignisziels. Nachdem Sie den EventBridgeAmazon-Zieltyp ausgewählt, einen Zielnamen eingegeben und die Veröffentlichung von Veranstaltungen aktiviert haben, wird ein Informationsfenster für den Amazon EventBridge Event Bus angezeigt.
2. Wählen Sie Weiter aus.
3. Wenn Sie auf dem Review-Bildschirm mit der Definition Ihres Veranstaltungsziels zufrieden sind, wählen SieHinzufügen eines Zielsaus. Dadurch wird die Übersichtsseite des Ereignisziels geöffnet, auf der ein Erfolgsbanner bestätigt, ob Ihr Ereignisziel erfolgreich erstellt oder geändert wurde.

Einrichten eines Amazon-Pinpoint-Ereignisziels für die Ereignisveröffentlichung

Ein Amazon Pinpoint Pinpoint-Ereignisziel benachrichtigt Sie über die E-Mail-Versandereignisse, die Sie in einem Konfigurationssatz angeben. Da ein Amazon Pinpoint Pinpoint-Ereignisziel nur in einem Konfigurationssatz eingerichtet werden kann, müssen Sie einen Konfigurationssatz erstellen, bevor Sie das Ereignisziel zum Konfigurationssatz hinzufügen.

Das Verfahren in diesem Abschnitt veranschaulicht, wie die Details zum Amazon-Pinpoint-Ereignisziel einem Konfigurationssatz hinzugefügt werden, und setzt voraus, dass Sie die Schritte 1 bis 6 unter Erstellen eines Ereignisziels abgeschlossen haben.

Sie können den UpdateConfigurationSetEventDestinationVorgang auch in der Amazon SES API V2 verwenden, um Ereignisziele zu erstellen und zu ändern.

Für die Arten von Kanälen, die Sie in Ihren Amazon-Pinpoint-Projekten konfiguriert haben, fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter Amazon-Pinpoint-Preise.

So fügen Sie einem Konfigurationssatz mithilfe der Konsole ein Amazon-Pinpoint-Ereignisziel hinzu

1. Dies sind die detaillierten Anweisungen zur Auswahl von Amazon Pinpoint als Ereigniszieltyp in Schritt 7. Es wird vorausgesetzt, dass Sie alle vorherigen Schritte in Erstellen eines Ereignisziels abgeschlossen haben.

   > **Note**
   >
   > Amazon Pinpoint unterstützt die Ereignistypen Delivery delays (Zustellungsverzögerungen) und Subscriptions (Abonnements) nicht.

   Nachdem Sie den Amazon Pinpoint-Zieltyp ausgewählt, einen Zielnamen eingegeben und die Veröffentlichung von Ereignissen aktiviert haben, wird der Bereich mit den Projektdetails von Amazon Pinpoint angezeigt. Die entsprechenden Felder werden in den folgenden Schritten behandelt.
2. Wählen Sie für Project (Projekt) ein vorhandenes Amazon-Pinpoint-Projekt aus oder wählen Sie Create a new project in Amazon Pinpoint (Neues Projekt in Amazon Pinpoint erstellen), um ein neues Projekt zu erstellen.

   Weitere Informationen zum Erstellen eines Projekts finden Sie unter Ein Projekt erstellen im Benutzerhandbuch zu Amazon Pinpoint.
3. Wählen Sie Weiter aus.
4. Wenn Sie auf dem Review-Bildschirm mit der Definition Ihres Veranstaltungsziels zufrieden sind, wählen SieHinzufügen eines Zielsaus. Dadurch wird die Übersichtsseite des Ereignisziels geöffnet, auf der ein Erfolgsbanner bestätigt, ob Ihr Ereignisziel erfolgreich erstellt oder geändert wurde.

Einrichten eines Amazon SNS-Ereignisziels für die Ereignisveröffentlichung

Ein Amazon SNS SNS-Ereignisziel benachrichtigt Sie über die E-Mail-Versandereignisse, die Sie in einem Konfigurationssatz angeben. Da ein Amazon SNS SNS-Ereignisziel nur in einem Konfigurationssatz eingerichtet werden kann, müssen Sie einen Konfigurationssatz erstellen, bevor Sie das Ereignisziel zum Konfigurationssatz hinzufügen.

Das Verfahren in diesem Abschnitt veranschaulicht, wie die Details zum Amazon-SNS-Ereignisziel einem Konfigurationssatz hinzugefügt werden, und setzt voraus, dass Sie die Schritte 1 bis 6 unter Erstellen eines Ereignisziels abgeschlossen haben.

Sie können den UpdateConfigurationSetEventDestinationVorgang auch in der Amazon SES API V2 verwenden, um Ereignisziele zu erstellen und zu ändern.

> **Note**
>
> Feedback-Benachrichtigungen für Unzustellbarkeiten, Beschwerden und Zustellungen können auch über Amazon SNS für jede Ihrer verifizierten Sendeidentitäten eingerichtet werden. Weitere Informationen finden Sie unter the section called “Konfigurieren von Amazon-SNS-Benachrichtigungen”.

Für das Senden von Nachrichten an die Endpunkte, die für Ihre Amazon SNS-Themen abonniert sind, fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter Amazon SNS-Preise.

So fügen Sie einem Konfigurationssatz mithilfe der Konsole ein Amazon SNS-Ereignisziel hinzu

1. Dies sind die detaillierten Anweisungen zur Auswahl von Amazon SNS als Ereigniszieltyp in Schritt 7. Es wird vorausgesetzt, dass Sie alle vorherigen Schritte in Erstellen eines Ereignisziels abgeschlossen haben. Nachdem Sie den Amazon SNS SNS-Zieltyp ausgewählt, einen Zielnamen eingegeben und die Veröffentlichung von Ereignissen aktiviert haben, wird der Themenbereich Amazon Simple Notification Service (SNS) angezeigt, dessen Felder in den folgenden Schritten behandelt werden.
2. Wählen Sie unter SNS Topic (SNS-Thema) ein vorhandenes Amazon SNS-Thema oder aber Create SNS topic (SNS-Thema erstellen) aus, um ein neues Thema zu erstellen.

   Weitere Informationen finden Sie unter Create a Topic (Ein Thema erstellen) im Entwicklerhandbuch zu Amazon Simple Notification Service.

   > **Important**
   >
   > Wenn Sie Ihr Thema mit Amazon SNS erstellen, wählen Sie für Type (Typ) nur Standard aus. (SES unterstützt keine FIFO-Typ-Themen.)

3. Wählen Sie Weiter aus.

4. Wenn Sie auf dem Review-Bildschirm mit der Definition Ihres Veranstaltungsziels zufrieden sind, wählen SieHinzufügen eines Zielsaus. Dadurch wird die Übersichtsseite des Ereignisziels geöffnet, auf der ein Erfolgsbanner bestätigt, ob Ihr Ereignisziel erfolgreich erstellt oder geändert wurde.
5. Unabhängig davon, ob Sie ein neues SNS-Thema erstellen oder ein vorhandenes auswählen, müssen Sie den Zugriff auf SES gewähren, um Benachrichtigungen für das Thema zu veröffentlichen. Wählen Sie auf der Zusammenfassungsseite des Ereignisziels aus dem vorherigen Schritt Amazon SNS aus der Spalte Destination type (Zieltyp) aus. Dadurch gelangen Sie zu Topics (Themen) in der Konsole von Amazon Simple Notification Service. Führen Sie die folgenden Schritte über die Amazon-SNS-Konsole aus:

   a. Wählen Sie den Namen des SNS-Themas aus, das Sie im vorherigen Schritt erstellt oder geändert haben.
   b. Wählen Sie auf dem Detailbildschirm des Themas Edit (Bearbeiten) aus.
   c. Um SES die Berechtigung zum Veröffentlichen von Benachrichtigungen für das Thema zu erteilen, erweitern Sie auf dem Bildschirm Edit topic (Thema bearbeiten) der SNS-Konsole die Access policy (Zugriffsrichtlinie) und fügen Sie im JSON editor (JSON-Editor) die folgende Berechtigungsrichtlinie hinzu:

      JSON

```
{
    "Version":"2012-10-17",
    "Id": "notification-policy",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "sns:Publish",
            "Resource": "arn:aws:sns:us-east-1:111122223333:topic_name",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "111122223333",
                    "AWS:SourceArn":
 "arn:aws:ses:topic_region:111122223333:configuration-set/configuration-
set-name"
                }
```

```
            }
        }
    ]
}
```

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- Ersetzen Sie es *topic_region* durch die AWS Region, in der Sie das SNS-Thema erstellt haben.
- Ersetzen Sie es *111122223333* durch Ihre AWS Konto-ID.
- *topic_name*Ersetzen Sie es durch den Namen Ihres SNS-Themas.
- *configuration-set-name*Ersetzen Sie es durch den Namen Ihres Konfigurationssatzes, der dem SNS-Ereignisziel zugeordnet ist.

d. Wählen Sie Änderungen speichern aus.

Schritt 3: Festlegen eines Konfigurationssatzes für das Senden von E-Mail

Nach dem Erstellen eines Konfigurationssatzes und dem Hinzufügen eines Ereignisziels besteht der letzte Schritt zur Ereignisveröffentlichung im Senden von E-Mails.

Damit Ereignisse im Zusammenhang mit einer E-Mail veröffentlicht werden, müssen Sie den Namen des Konfigurationssatzes angeben, der mit der E-Mail- verknüpft werden soll. Optional können Sie Tags zur Kategorisierung der E-Mail-Nachricht bereitstellen.

Diese Informationen stellen Sie Amazon SES entweder als Parameter an die E-Mail sendende API, als -spezifischer E-Mail-Header oder als benutzerdefinierter Header in Ihrer MIME-Nachricht bereit. Welche Methode Sie wählen, hängt von der Schnittstelle ab, mit der Sie E-Mails senden. Sehen Sie sich dazu die folgende Tabelle an.

Schnittstelle zum Senden von E-Mails	Möglichkeiten zum Veröffentlichen von Events
`SendEmail`	API-Parameter
`SendTemplatedEmail`	API-Parameter
`SendBulkTemplatedEmail`	API-Parameter

Schnittstelle zum Senden von E-Mails	Möglichkeiten zum Veröffentlichen von Events
`SendCustomVerificationEmail`	API-Parameter
`SendRawEmail`	API-Parameter, Amazon SES-spezifische E-Mail-Header oder benutzerdefinierte MIME-Header **Important** Wenn Sie Nachrichten-Tags sowohl mit Headern als auch mit API-Parametern angeben, verwendet Amazon SES nur die durch API-Parameter bereitgestellten Nachricht Tags. Amazon SES verknüpft keine Nachrichten-Tags, die durch API-Parameter und Header angegeben werden.
SMTP-Schnittstelle	Amazon SES-spezifische E-Mail-Header

In den folgenden Abschnitten wird beschrieben, wie Sie Konfigurationssätze und Nachrichten-Tags mithilfe von Headern und mithilfe von API-Parametern festlegen.

- Verwenden von Amazon SES-API-Parametern
- Verwenden von Amazon SES-spezifischen E-Mail-Headern
- Verwenden von benutzerdefinierten E-Mail-Headern

Note

Optional können Sie Nachrichten-Tags in den Kopfzeilen Ihrer E-Mails einschließen. Nachrichten-Tags können die Zahlen 0-9, die Buchstaben A-Z (Groß- und Kleinbuchstaben), Bindestriche (-) und Unterstriche (_) enthalten.

Verwenden von Amazon SES-API-Parametern

Um SendEmail,, SendTemplatedEmailSendBulkTemplatedEmailSendCustomVerificationEmail, oder SendRawEmailzusammen mit der Veröffentlichung von Ereignissen zu verwenden, geben Sie den Konfigurationssatz und die Nachrichten-Tags an, indem Sie die ConfigurationSetaufgerufenen Datenstrukturen MessageTagan den API-Aufruf übergeben.

Weitere Informationen zur Verwendung der Amazon SES API finden Sie unter Referenz zu Amazon Simple Email Service API.

Verwenden von Amazon SES-spezifischen E-Mail-Headern

Wenn Sie `SendRawEmail` oder die SMTP-Schnittstelle verwenden, können Sie den Konfigurationssatz und die Nachrichten-Tags angeben, indem Sie der E-Mail Amazon SES-spezifische Header hinzufügen. Vor dem Senden der E-Mail entfernt Amazon SES die Header. In der folgenden Tabelle sind die Namen der zu verwendenden Header aufgeführt.

Informationen der Ereignisveröffentlichung	Header
Konfigurationssatz	`X-SES-CONFIGURATION-SET`
Nachrichten-Tags	`X-SES-MESSAGE-TAGS`

Das folgende Beispiel zeigt, wie die Header in einer Raw-E-Mail aussehen können, die Sie an Amazon SES senden.

```
X-SES-MESSAGE-TAGS: tagName1=tagValue1, tagName2=tagValue2
X-SES-CONFIGURATION-SET: myConfigurationSet
From: sender@example.com
To: recipient@example.com
Subject: Subject
Content-Type: multipart/alternative;
 boundary="----=_boundary"

------=_boundary
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

body
------=_boundary
Content-Type: text/html; charset=UTF-8
```

```
Content-Transfer-Encoding: 7bit

body
------=_boundary--
```

Verwenden von benutzerdefinierten E-Mail-Headern

Sie müssen zwar den Namen des Konfigurationssatzes mit dem Amazon SES-spezifischen Header `X-SES-CONFIGURATION-SET` angeben, aber Sie können die Nachrichten-Tags mithilfe eigener MIME-Header festlegen.

> **Note**
>
> Die für die Amazon SES-Ereignisveröffentlichung verwendeten Header-Namen und -Werte müssen das ASCII-Format aufweisen. Wenn Sie einen Nicht-ASCII-Header-Namen oder -Wert für die Veröffentlichung von Amazon SES SES-Ereignissen angeben, ist der E-Mail-Versandaufruf trotzdem erfolgreich, aber die Ereignismetriken werden nicht an Amazon gesendet. CloudWatch

Arbeiten mit Amazon SES-Ereignisdaten

Nachdem Sie die Ereignisveröffentlichung eingerichtet und einen Konfigurationssatz für das Senden von E-Mails angegeben haben, können Sie Ihre E-Mail-Sendeereignisse aus dem Ereignisziel abrufen, die Sie beim Einrichten des Konfigurationsatzs im Zusammenhang mit der E-Mail angegeben haben.

In diesem Abschnitt wird beschrieben, wie Sie Ihre E-Mail-Sendeereignisse von Amazon CloudWatch und Amazon Data Firehose abrufen und wie Sie die von Amazon SNS bereitgestellten Ereignisdaten interpretieren.

- Amazon SES SES-Ereignisdaten werden abgerufen von CloudWatch
- Amazon SES SES-Ereignisdaten von Firehose abrufen
- Interpretieren von Amazon SES-Ereignisdaten aus Amazon SNS

Amazon SES SES-Ereignisdaten werden abgerufen von CloudWatch

Amazon SES kann Kennzahlen für Ihre E-Mail-Versandereignisse an Amazon veröffentlichen CloudWatch. Wenn Sie Ereignisdaten auf veröffentlichen CloudWatch, werden diese Metriken als

geordnete Reihe von Zeitreihendaten bereitgestellt. Sie können diese Metriken verwenden, um die Leistung des E-Mail-Versands zu überwachen. Sie können beispielsweise die Beschwerdekennzahl überwachen und einen CloudWatch Alarm einrichten, der ausgelöst wird, wenn die Kennzahl einen bestimmten Wert überschreitet.

Es gibt zwei Granularitätsebenen, auf denen Amazon SES diese Ereignisse veröffentlichen kann: CloudWatch

- Across your AWS-Konto — Diese groben Kennzahlen, die den Metriken entsprechen, die Sie mit der Amazon SES SES-Konsole und der `GetSendStatistics` API überwachen, sind Gesamtwerte für Ihr gesamtes AWS-Konto System. Amazon SES veröffentlicht diese Metriken CloudWatch automatisch.
- Fine-grained – Diese Metriken werden anhand von E-Mail-Eigenschaften kategorisiert, die Sie mithilfe von Nachrichten-Tags definieren. Um diese Metriken zu veröffentlichen CloudWatch, müssen Sie die Veröffentlichung von Ereignissen mit einem CloudWatch Veranstaltungsziel einrichten und beim Senden einer E-Mail einen Konfigurationssatz angeben. Sie können auch Nachrichten-Tags angeben oder automatische Tags verwenden, die Amazon SES automatisch bereitstellt.

In diesem Abschnitt werden die verfügbaren Metriken beschrieben und wie Sie in CloudWatch angezeigt werden.

Verfügbare Metriken

Sie können die folgenden Amazon SES SES-Metriken zum Senden von E-Mails veröffentlichen an CloudWatch:

- Send (Senden) – die Sendeanfrage war erfolgreich und Amazon SES versucht, dem E-Mail-Server des Empfängers die Nachricht zuzustellen. (Wenn eine Unterdrückung auf Kontoebene oder eine globale Unterdrückung verwendet wird, zählt SES sie weiterhin als Senden, aber die Zustellung wird unterdrückt.)
- RenderingFailure— Die E-Mail wurde aufgrund eines Problems beim Rendern der Vorlage nicht gesendet. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail-Vorlage mithilfe der `SendTemplatedEmail`- oder `SendBulkTemplatedEmail`-API-Operationen senden.
- Rejects (Ablehnungen) – Amazon SES hat die E-Mail akzeptiert, aber festgestellt, dass sie einen Virus enthielt und nicht versucht hat, ihn an den Mail-Server des Empfängers zu übermitteln.

- Delivery (Zustellung) – Amazon SES hat die E-Mail erfolgreich an den Mail-Server des Empfängers übermittelt.
- Bounce – eine permanente Unzustellbarkeit, sodass die E-Mail vom E-Mail-Server des Empfängers dauerhaft abgelehnt wurde. (Soft Bounces sind nur enthalten, wenn SES nicht mehr versucht, die E-Mail zuzustellen. Im Allgemeinen deuten diese Soft Bounces auf einen Zustellungsfehler hin, obwohl in einigen Fällen ein Soft Bounce auch dann zurückgegeben werden kann, wenn die E-Mail den Posteingang des Empfängers erfolgreich erreicht hat. Dies tritt normalerweise auf, wenn der Empfänger eine out-of-office automatische Antwort sendet. In diesem AWS re:POST-Artikel erfährst du mehr über Soft Bounces.)
- Complaint (Beschwerde) – die E-Mail wurde erfolgreich an den E-Mail-Server des Empfängers gesendet, der Empfänger hat sie jedoch als Spam markiert.
- DeliveryDelay— Die E-Mail konnte nicht an den Mailserver des Empfängers zugestellt werden, da ein vorübergehendes Problem aufgetreten ist. Verzögerungen bei der Zustellung können, z. B. auftreten, wenn der Posteingang des Empfängers voll ist oder der empfangende E-Mail-Server ein vorübergehendes Problem aufweist.
- Subscription (Abonnement) – die E-Mail wurde erfolgreich zugestellt, aber der Empfänger hat die Abonnementeinstellungen aktualisiert, indem er auf `List-Unsubscribe` in der E-Mail-Kopfzeile oder auf den `Unsubscribe`-Link in der Fußzeile geklickt hat.
- Open (Geöffnet) – der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
- Click (Klick) – der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.

Verfügbare Dimensionen

CloudWatch verwendet die Dimensionsnamen, die Sie angeben, wenn Sie einem Konfigurationssatz in Amazon SES ein CloudWatch Ereignisziel hinzufügen. Weitere Informationen finden Sie unter Richten Sie ein CloudWatch Veranstaltungsziel für die Veröffentlichung von Veranstaltungen ein.

Amazon SES SES-Metriken in der CloudWatch Konsole anzeigen

Das folgende Verfahren beschreibt, wie Sie Ihre Amazon SES SES-Eventveröffentlichungsmetriken mithilfe der CloudWatch Konsole anzeigen können.

So zeigen Sie Metriken mit der CloudWatch Konsole an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.

2. Ändern Sie, falls erforderlich, die Region. Wählen Sie in der Navigationsleiste die Region aus, in der sich Ihre AWS Ressourcen befinden. Weitere Informationen finden Sie unter -Regionen und Endpunkte.
3. Wählen Sie im Navigationsbereich Alle Metriken aus.
4. Wählen Sie im Bereich Metriken SES aus.
5. Wählen Sie die Metrik aus, die Sie anzeigen möchten. Zum Anzeigen von präzisen Metriken für die Ereignisveröffentlichung wählen Sie die Kombination von Dimensionen, die Sie angegeben haben, als Sie Ihr CloudWatch-Ereignisziel eingerichtet haben. Weitere Informationen zum Anzeigen von Metriken mit CloudWatch finden Sie unter CloudWatchAmazon-Metriken verwenden.

Um Metriken mit dem anzuzeigen AWS CLI

- Geben Sie in einer Eingabeaufforderung den folgenden Befehl ein:

```
aws cloudwatch list-metrics --namespace "AWS/SES"
```

Amazon SES SES-Ereignisdaten von Firehose abrufen

Amazon SES veröffentlicht E-Mail-Sendeereignisse an Firehose als JSON-Datensätze. Firehose veröffentlicht die Datensätze dann an dem AWS Serviceziel, das Sie bei der Einrichtung des Lieferdatenstroms in Firehose ausgewählt haben. Informationen zur Einrichtung von Firehose-Lieferdatenströmen finden Sie unter Creating an Firehose Delivery Stream im Amazon Data Firehose Developer Guide.

Themen in diesem Abschnitt:

- Inhalt der Ereignisdaten, die Amazon SES auf Firehose veröffentlicht
- Beispiele für Ereignisdaten, die Amazon SES auf Firehose veröffentlicht

Inhalt der Ereignisdaten, die Amazon SES auf Firehose veröffentlicht

Amazon SES veröffentlicht Aufzeichnungen über E-Mail-Versandereignisse an Amazon Data Firehose im JSON-Format. Bei der Veröffentlichung von Ereignissen in Firehose folgt Amazon SES jedem JSON-Datensatz mit einem Zeilenumbruchzeichen.

Beispieldatensätze für all diese Benachrichtigungstypen finden Sie unter Beispiele für Ereignisdaten, die Amazon SES auf Firehose veröffentlicht.

Themen in diesem Abschnitt

- JSON-Objekt der obersten Ebene
- Mail-Objekt
- Bounce-Objekt
- Complaint-Objekt
- Delivery-Objekt
- Send-Objekt
- Reject-Objekt
- Open-Objekt
- Click-Objekt
- Rendering-Failure-Objekt
- DeliveryDelay Objekt
- Abonnementobjekt

JSON-Objekt der obersten Ebene

Das JSON-Objekt der obersten Ebene in einem E-Mail-Sendeereignisdatensatz enthält die folgenden Felder.

Feldname	Description
`eventType`	Eine Zeichenfolge, die die Art des Ereignisses angibt. Mögliche Werte: `Bounce`, `Complaint`, `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure`, `DeliveryDelay` oder `Subscription`. Wenn Sie keine Ereignisveröffentlichung einrichten heißt dieses Feld `notificationType`.

Feldname	Description
`mail`	Ein JSON-Objekt, das Informationen über die E-Mail enthält, die das Ereignis hervorgerufen hat.
`bounce`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Bounce` eingestellt ist. Es enthält Informationen über die Unzustellbarkeit.
`complaint`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Complaint` eingestellt ist. Es enthält Informationen über die Beschwerde.
`delivery`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Delivery` eingestellt ist. Es enthält Informationen über die Zustellung.
`send`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Send` eingestellt ist.
`reject`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Reject` eingestellt ist. Es enthält Informationen über die Ablehnung.
`open`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Open` eingestellt ist. Es enthält Informationen über das offene Ereignis.
`click`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Click` eingestellt ist. Es enthält Informationen über das Klick-Ereignis.
`failure`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Rendering Failure` eingestellt ist. Es enthält Informationen über das Rendering-Fehlerereignis.

Feldname	Description
`deliveryDelay`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `DeliveryDelay` eingestellt ist. Es enthält Informationen zur verzögerten Zustellung einer E-Mail.
`subscription`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Subscription` eingestellt ist. Es enthält Informationen zu den Abonnementeinstellungen.

Mail-Objekt

Jeder E-Mail-Sendeereignisprotokolleintrag enthält Informationen über die ursprüngliche E-Mail im `mail`-Objekt. Das JSON-Objekt enthält Informationen über ein `mail`-Objekt mit den folgenden Feldern.

Feldname	Description
`timestamp`	Datum und Uhrzeit im ISO8601 Format (YYYY-MM DDThh -:mm:ss.sz), an dem die Nachricht gesendet wurde.
`messageId`	Eine eindeutige ID, die Amazon SES der Nachricht zugewiesen hat. Amazon SES gibt diesen Wert an Sie zurück, wenn Sie die Nachricht gesendet haben. **Note** Diese Nachrichten-ID wurde von Amazon SES zugewiesen. Sie finden diese Mitteilungs-ID in der ursprünglichen E-Mail in den Feldern `headers`

Feldname	Description
	und `commonHeaders` des Objekts `mail`.
`source`	Die E-Mail-Adresse, von der die Nachricht gesendet wurde (die Envelope-MAIL-FROM-Adresse).
`sourceArn`	Der Amazon-Ressourcenname (ARN) der Identität, die zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt `sourceArn` den ARN der ID an, die – gemäß Autorisierung durch den Identitätsbesitzer – vom stellvertretenden Sender zum Senden der E-Mail verwendet werden soll. Weitere Informationen zur Sendeautorisierung finden Sie unter E-Mail-Authentifizierungsmethoden.
`sendingAccountId`	Die AWS Konto-ID des Kontos, das zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt `sendingAccountId` die Konto-ID des stellvertretenden Senders an.
`destination`	Eine Liste der E-Mail-Adressen, an die die ursprüngliche E-Mail gesendet wurde.
`headersTruncated`	Eine Zeichenfolge, die angibt, ob die Header in der Benachrichtigung abgeschnitten sind. Dies passiert, wenn die Header größer als 10 KB sind. Mögliche Werte sind `true` und `false`.

Feldname	Description
`headers`	Eine Liste der ursprünglichen Header der E-Mail. Jeder Header in der Liste verfügt über die Felder `name` und `value`. **Note** Jede Nachrichten-ID im Feld `headers` stammt von der ursprünglichen Nachricht, die Sie an Amazon SES übergeben haben. Die Nachrichten-ID, die Amazon SES der Nachricht später zugewiesen hat, befindet sich im Feld `messageId` des Objekts `mail`.
`commonHeaders`	Eine Zuordnung der ursprünglichen, häufig verwendeten Header der E-Mail. **Note** Die Nachrichten-ID im Feld `commonHeaders` ist die Nachrichten-ID, die Amazon SES der Nachricht später im Feld `messageId` des Objekts `mail` zugewiesen hat.
`tags`	Eine Liste von Tags, die der E-Mail-Adresse zugeordnet sind.

Bounce-Objekt

Das JSON-Objekt, das die Informationen zu einem `Bounce`-Ereignis enthält, weist immer die folgenden Felder auf.

Feldname	Description
`bounceType`	Der Unzustellbarkeitstyp, wie er von Amazon SES festgelegt wurde.
`bounceSubType`	Der untergeordnete Typ der Unzustellbarkeit, wie er von Amazon SES festgelegt wurde.
`bouncedRecipients`	Eine Liste mit Informationen über die Empfänger der ursprünglichen E-Mail, an die diese nicht zugestellt werden konnte.
`timestamp`	Datum und Uhrzeit im ISO8601 Format (YYYY-MM-:mm:ss.sz DDThh), an dem der ISP die Bounce-Benachrichtigung gesendet hat.
`feedbackId`	Eine eindeutige ID für die Unzustellbarkeit.
`reportingMTA`	Der Wert des `Reporting-MTA` -Felds der DSN. Dies ist der Wert der Message Transfer Authority (MTA), die versucht hat, die Zustellungs-, Weiterleitungs- oder Gateway-Operation durchzuführen, die in der DSN beschrieben ist. **Note** Dieses Feld wird nur dann angezeigt, wenn eine Zustellungsstatusbenachrichtigung (Delivery Status Notification, DNS) an die Unzustellbarkeitsbenachrichtigung angehängt wurde.

Empfänger, an die nicht zugestellt werden konnte

Ein Unzustellbarkeitsereignis kann für einen einzelnen Empfänger oder für mehrere Empfänger gelten. Das `bouncedRecipients`-Feld enthält eine Liste von Objekten – eines pro Empfänger, für den das Bounce-Ereignis auftritt – und weist zusätzlich immer das folgende Feld auf.

Feldname	Description
`emailAddress`	Die E-Mail-Adresse des Empfängers. Ist eine DSN verfügbar, ist dies der Wert des `Final-Recipient` -Felds der DSN.

Wurde eine DSN an eine Unzustellbarkeitsbenachrichtigung angehängt, sind möglicherweise folgende Felder ebenfalls vorhanden.

Feldname	Description
`action`	Der Wert des `Action`-Felds der DSN. Es zeigt die Aktion an, die von der berichtenden MTA als Reaktion auf die gescheiterte Zustellung der Benachrichtigung an diesen Empfänger ausgeführt wurde.
`status`	Der Wert des `Status`-Felds der DSN. Dies ist der vom Transport unabhängige Statuscode pro Empfänger, der den Zustellstatus der Nachricht anzeigt.
`diagnosticCode`	Der vom berichtenden MTA gemeldete Statuscode. Dies ist der Wert des `Diagnostic-Code` -Felds der DSN. Dieses Feld ist möglicherweise nicht im DSN und daher auch nicht in JSON enthalten.

Unzustellbarkeitstypen

Jedes Unzustellbarkeitsereignis ist von einem der Typen, die in der folgenden Tabelle gezeigt werden.

Das System zur Ereignisveröffentlichung veröffentlicht nur permanente Unzustellbarkeiten und temporäre Unzustellbarkeiten, die nicht mehr von Amazon SES abgerufen werden. Wenn Sie Unzustellbarkeitsnachrichten erhalten, die mit `Permanent` gekennzeichnet sind, sollten Sie die

entsprechenden E-Mail-Adressen aus Ihrer Mailingliste entfernen; Sie werden in Zukunft nicht mehr an sie senden können. `Transient`-Unzustellbarkeitsnachrichten werden an Sie gesendet, wenn eine Nachricht mehrmals temporär unzustellbar war und Amazon SES nicht mehr versucht, sie erneut zu senden. Es ist möglich, dass das erneute Senden einer E-Mail an eine Adresse später erfolgreich ist, die ursprünglich zu einem `Transient`-Bounce führte.

bounceType	bounceSubType	Description
`Undetermined`	`Undetermined`	Amazon SES konnte keinen bestimmten Grund für das Scheitern der Zustellung finden.
`Permanent`	`General`	Amazon SES hat eine allgemeine permanente Unzustellbarkeit erhalten. Wenn Sie diese Art von Unzustellbarkeit erhalten, sollten Sie die E-Mail-Adresse des Empfängers aus Ihrer Mailing-Liste entfernen.
`Permanent`	`NoEmail`	Amazon SES hat eine Benachrichtigung über eine permanente Unzustellbarkeit enthalten, da die Ziel-E-Mail-Adresse nicht existiert. Wenn Sie diese Art von Unzustellbarkeit erhalten, sollten Sie die E-Mail-Adresse des Empfängers aus Ihrer Mailing-Liste entfernen.
`Permanent`	`Suppressed`	Amazon SES hat das Senden an diese Adresse unterdrückt, da bereits mehrere Zustellversuche aufgrund einer ungültigen Adresse fehlgeschlagen sind. Informationen zum Überschreiben der globalen Unterdrückungsliste finden Sie unterVerwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole.
`Permanent`	`OnAccountSuppressionList`	Amazon SES hat das Senden an diese Adresse unterdrückt, da sie sich auf der Unterdrückungsliste auf Kontoebene befindet.

bounceType	bounceSubType	Description
		Dies zählt nicht für Ihre Unzustellbarkeitsraten-Metrik.
`Transient`	`General`	Amazon SES hat eine allgemeine Unzustellbarkeitsbenachrichtigung erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger zukünftig möglich.
`Transient`	`MailboxFull`	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung erhalten, weil das Postfach voll ist. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger zukünftig möglich.
`Transient`	`MessageTooLarge`	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung aufgrund einer zu großen E-Mail erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie die Größe der Nachricht reduzieren.
`Transient`	`CustomTimeoutExceeded`	Amazon SES war nicht in der Lage, die E-Mail innerhalb der vom E-Mail-Absender angegebenen Zeit erfolgreich zuzustellen. (In der Bounce-Nachricht wird der Grund für mögliche fehlgeschlagene Zustellungsversuche innerhalb der definierten TTL angegeben.)
`Transient`	`ContentRejected`	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung aufgrund eines abgelehnten Inhalts erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie den Inhalt der Nachricht ändern.

bounceType	bounceSubType	Description
`Transient`	`AttachmentRejected`	Amazon SES hat eine Unzustellbarkeitsb enachrichtigung aufgrund eines abgelehnten Anhangs erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie den Anhang entfernen oder ändern.

Complaint-Objekt

Das JSON-Objekt enthält Informationen über ein `Complaint`-Ereignis mit den folgenden Feldern.

Feldname	Description
`complainedRecipients`	Eine Liste mit Informationen zu Empfängern, die sich möglicherweise beschwert haben.
`timestamp`	Datum und Uhrzeit im ISO8601 Format (YYYY-MM DDThh -:mm:ss.sz), an dem der ISP die Beschwerdebenachrichtigung gesendet hat.
`feedbackId`	Eine eindeutige ID für die Beschwerde.
`complaintSubType`	Der Untertyp der Beschwerde, wie von Amazon SES festgelegt.

Ist zudem ein Feedback-Bericht an die Beschwerde angehängt, sind möglicherweise die folgenden Felder vorhanden.

Feldname	Description
`userAgent`	Der Wert des `User-Agent` -Felds aus dem Feedback-Bericht. Gibt den Namen und die Version des Systems an, das den Bericht generiert hat.

Feldname	Description
`complaintFeedbackType`	Der Wert des `Feedback-Type` -Felds aus dem Feedback-Bericht, der vom ISP empfangen wurde. Enthält die Art des Feedbacks.
`arrivalDate`	Der Wert des *`Received-Date`* Felds *`Arrival-Date`* oder aus dem Feedback-Bericht im Format (YYYY-MM-:mm:ss.sz). ISO8601 DDThh Dieses Feld ist möglicher weise nicht im Bericht und daher auch nicht in JSON enthalten.

Empfänger, die sich beschwert haben

Das `complainedRecipients`-Feld enthält eine Liste von Empfängern, die sich möglicherweise beschwert haben.

> **Important**
>
> Da die meisten ISPs die E-Mail-Adresse des Empfängers, der die Beschwerde eingereicht hat, aus der Beschwerdebenachrichtigung herauslesen, enthält diese Liste Informationen über Empfänger, die die Beschwerde möglicherweise gesendet haben, basierend auf den Empfängern der ursprünglichen Nachricht und dem ISP, von dem wir die Beschwerde erhalten haben. Amazon SES führt einen Abgleich mit der ursprünglichen Nachricht durch, um diese Empfängerliste festzulegen.

JSON-Objekte in dieser Liste enthalten das folgende Feld.

Feldname	Description
`emailAddress`	Die E-Mail-Adresse des Empfängers.

Beschwerdetypen

Sie sehen möglicherweise die folgenden Beschwerdetypen im `complaintFeedbackType`-Feld, so wie sie vom meldenden ISP entsprechend der Website zu Internet Assigned Numbers Authority zugewiesen wurden:

Feldname	Description
`abuse`	Weist auf unerwünschte E-Mails oder eine andere Art von E-Mail-Missbrauch hin.
`auth-failure`	Bericht über einen E-Mail-Authentifizierungsfehler.
`fraud`	Weist auf einen Betrug oder Phishing hin.
`not-spam`	Weist darauf hin, dass die Entität, die den Bericht bereitstellt, die Nachricht nicht als Spam betrachtet. Dies kann verwendet werden, um eine Nachricht zu korrigieren, die fälschlicherweise als Spam gekennzeichnet oder kategorisiert wurde.
`other`	Gibt eine andere Art von Feedback an, das nicht zu den registrierten Typen passt.
`virus`	Meldet, dass in der ursprünglichen Nachricht ein Virus entdeckt wurde.

Delivery-Objekt

Das JSON-Objekt, das die Informationen zu einem `Delivery`-Ereignis enthält, weist immer die folgenden Felder auf.

Feldname	Description
`timestamp`	Datum und Uhrzeit der Zustellung der E-Mail an den E-Mail-Server des Empfängers durch

Feldname	Description
	Amazon SES im ISO8601 Format (YYYY-MM-: mm:ss.sz). DDThh
`processingTimeMillis`	Die Zeit in Millisekunden zwischen dem Zeitpunkt, als Amazon SES die Anforderu ng des Senders angenommen hat, und dem Zeitpunkt, als die Nachricht an den Mail-Server des Empfängers übergeben hat.
`recipients`	Eine Liste der beabsichtigten Empfänger, für die das Übermittlungsereignis gilt.
`smtpResponse`	Die SMTP-Antwort des Remote-ISPs, der die E-Mail von Amazon SES zugelassen hat. Diese Nachricht variiert je nach E-Mail, empfangen dem Mail-Server und empfangendem ISP.
`reportingMTA`	Der Hostname des Amazon SES-Mail-Servers, der die E-Mail gesendet hat.
`remoteMtaIp`	Die IP-Adresse der MTA, an die Amazon SES die E-Mail zugestellt hat.

Send-Objekt

Das JSON-Objekt mit Informationen über das `send`-Ereignis ist immer leer.

Reject-Objekt

Das JSON-Objekt, das die Informationen zu einem `Reject`-Ereignis enthält, weist immer die folgenden Felder auf.

Feldname	Description
`reason`	Der Grund für die Ablehnung der E-Mail. Der einzige mögliche Wert ist `Bad content`. Er bedeutet, dass Amazon SES erkannt hat,

Feldname	Description
	dass die E-Mail einen Virus enthält. Wenn eine Nachricht abgelehnt wird, hält Amazon SES ihre Verarbeitung an und versucht nicht, sie dem E-Mail-Server des Empfängers zuzustellen.

Open-Objekt

Das JSON-Objekt, das die Informationen zu einem `0pen`-Ereignis enthält, enthält immer die folgenden Felder.

Feldname	Description
`ipAddress`	Die IP-Adresse des Empfängers.
`timestamp`	Datum und Uhrzeit des Auftretens des Öffnungsereignisses im Format (YYYY-MM-:mm:ss.sz). ISO8601 DDThh
`userAgent`	Der Benutzeragent des Geräts oder E-Mail-Client, mit dem der Empfänger die E-Mail geöffnet hat.

Click-Objekt

Das JSON-Objekt, das die Informationen zu einem `Click`-Ereignis enthält, enthält immer die folgenden Felder.

Feldname	Description
`ipAddress`	Die IP-Adresse des Empfängers.
`timestamp`	Datum und Uhrzeit des Auftretens des Klickereignisses im Format (YYYY-MM-:mm:ss.sz). ISO8601 DDThh

Feldname	Description
`userAgent`	Der Benutzeragent des Clients, den der Empfänger zum Klicken auf einen Link in der E-Mail verwendet hat.
`link`	Die URL des Links, auf den der Empfänger geklickt hat.
`linkTags`	Eine Liste der Tags, die dem Link mithilfe des `ses:tags`-Attributs hinzugefügt wurden. Weitere Informationen zum Hinzufügen von Tags zu Links in Ihren E-Mails finden Sie unter F5. Kann ich Links mit eindeutigen Bezeichnern markieren? in den Amazon SES SES-Metriken zum Senden von E-Mails FAQs.

Rendering-Failure-Objekt

Das JSON-Objekt enthält Informationen über ein `Rendering Failure`-Ereignis mit den folgenden Feldern.

Feldname	Description
`templateName`	Der Name der Vorlage, die zum Senden der E-Mail verwendet wurde.
`errorMessage`	Eine Nachricht, die weitere Informationen über den Rendering-Fehler enthält.

DeliveryDelay Objekt

Das JSON-Objekt enthält Informationen über ein `DeliveryDelay`-Ereignis mit den folgenden Feldern.

Feldname	Description
`delayType`	Die Art der Verzögerung. Die möglichen Werte sind: • InternalFailure— Ein internes Amazon SES SES-Problem führte zu einer Verzögerung der Nachricht. • General – ein generischer Fehler ist während der SMTP-Konversation aufgetreten. • MailboxFull— Das Postfach des Empfängers ist voll und kann keine weiteren Nachrichten empfangen. • SpamDetected— Der E-Mail-Server des Empfängers hat eine große Menge unerwünschter E-Mails von Ihrem Konto erkannt. • RecipientServerError— Ein vorüberge hendes Problem mit dem E-Mail-Server des Empfängers verhindert die Zustellung der Nachricht. • IPFailure— Die IP-Adresse, über die die Nachricht gesendet wird, wird vom E-Mail-Anbieter des Empfängers blockiert oder gedrosselt. • TransientCommunicationFailure— Während der SMTP-Konversation mit dem E-Mail-Anbieter des Empfängers ist ein vorüberge hender Kommunikationsfehler aufgetreten. • BYOIPHostNameLookupUnavailable— Amazon SES konnte den DNS-Hostnamen für Ihre IP-Adressen nicht ermitteln. Diese Art von Verzögerung tritt nur auf, wenn Sie Bring Your Own IP verwenden.

Feldname	Description
	• Unbestimmt – Amazon SES konnte den Grund für die Lieferverzögerung nicht ermitteln. • SendingDeferral— Amazon SES hat es für angemessen erachtet, die Nachricht intern zu verschieben.
`delayedRecipients`	Ein Objekt, das Informationen zum E-Mail-Empfänger enthält
`expirationTime`	Das Datum und die Uhrzeit, wann Amazon SES die Zustellung der Nachricht nicht mehr versucht. Dieser Wert wird im ISO 8601-Format angezeigt.
`reportingMTA`	Die IP-Adresse des Message Transfer Agent (MTA), der die Verzögerung gemeldet hat
`timestamp`	Datum und Uhrzeit, wann die Verzögerung aufgetreten ist (im ISO 8601-Format)

Empfänger, an die verzögert zugestellt wurde

Das `delayedRecipients`-Objekt enthält die folgenden Werte:

Feldname	Description
`emailAddress`	Die E-Mail-Adresse, die zu einer verzögerten Zustellung der Nachricht führte
`status`	Der SMTP-Statuscode, der der Zustellverzögerung zugeordnet ist
`diagnosticCode`	Der Diagnosecode, der vom empfangenden Message Transfer Agent (MTA) bereitgestellt wird

Abonnementobjekt

Das JSON-Objekt enthält Informationen über ein `Subscription`-Ereignis mit den folgenden Feldern.

Feldname	Description
`contactList`	Der Name der Liste, auf der sich der Kontakt befindet.
`timestamp`	Datum und Uhrzeit im ISO8601 Format (YYYY-MM DDThh -:mm:ss.sz), an dem der ISP die Abonnementbenachrichtigung gesendet hat.
`source`	Die E-Mail-Adresse, von der die Nachricht gesendet wurde (die Envelope-MAIL-FROM-Adresse).
`newTopicPreferences`	Eine JSON-Datenstruktur (Zuweisung), die den Abonnementstatus aller Themen in der Kontaktliste angibt, die den Status nach einer Änderung (Kontakt abonniert oder Abonnement abbestellt) anzeigt.
`oldTopicPreferences`	Eine JSON-Datenstruktur (Zuweisung), die den Abonnementstatus aller Themen in der Kontaktliste angibt, die den Status vor der Änderung (Kontakt abonniert oder Abonnement abbestellt) anzeigt.

Einstellungen für neue/alte Themen

Die Objekte `newTopicPreferences` und `oldTopicPreferences` enthalten die folgenden Werte.

Feldname	Description
`unsubscribeAll`	Gibt an, ob der Kontakt das Abonnement von allen Themen in der Kontaktliste abbestellt hat.

Feldname	Description
`topicSubscriptionStatus`	Gibt den Abonnementstatus des Themas in dem `topicName` Feld an, das angibt, ob es derzeit für den Empfang von Benachric htigungen von SES für den angegebenen Ereignistyp angemeldet ist. Mögliche Werte sind OptIn(abonniert) oder OptOut(abgemeldet) in dem Feld. `subscriptionStatus`
`topicDefaultSubscriptionStatus`	Gibt den Standard-Abonnementstatus des Themas im `topicName` Feld an, der bestimmt, ob neue Themen, die dem Veranstal tungsziel hinzugefügt werden, standardmäßig abonniert oder abgemeldet werden. Mögliche Werte sind OptIn(standardmäßig abonniert) oder OptOut(standardmäßig abgemeldet) im Feld. `subscriptionStatus`

Beispiele für Ereignisdaten, die Amazon SES auf Firehose veröffentlicht

Dieser Abschnitt enthält Beispiele für die Arten von E-Mail-Versandereignissen, die Amazon SES in Firehose veröffentlicht.

Themen in diesem Abschnitt:

- Bounce-Datensatz
- Complaint-Datensatz
- Delivery-Datensatz
- Send-Datensatz
- Reject-Datensatz
- Open-Datensatz
- Click-Datensatz
- Rendering Failure-Datensatz
- DeliveryDelay aufzeichnen
- Abonnementdatensatz

> **Note**
>
> In den folgenden Beispielen wird, wenn ein `tag`-Feld verwendet wird, Ereignisveröffentlichung durch einen Konfigurationssatz verwendet, für den SES die Veröffentlichung von Tags für alle Ereignistypen unterstützt. Wenn Sie Feedback-Benachrichtigungen direkt über die Identität verwenden, veröffentlicht SES keine Tags. Lesen Sie mehr über das Hinzufügen von Tags, wenn Sie einen Konfigurationssatz erstellen oder einen Konfigurationssatz ändern.

Bounce-Datensatz

Im Folgenden finden Sie ein Beispiel für einen `Bounce` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType":"Bounce",
  "bounce":{
    "bounceType":"Permanent",
    "bounceSubType":"General",
    "bouncedRecipients":[
      {
        "emailAddress":"recipient@example.com",
        "action":"failed",
        "status":"5.1.1",
        "diagnosticCode":"smtp; 550 5.1.1 user unknown"
      }
    ],
    "timestamp":"2017-08-05T00:41:02.669Z",
    "feedbackId":"01000157c44f053b-61b59c11-9236-11e6-8f96-7be8aexample-000000",
    "reportingMTA":"dsn; mta.example.com"
  },
  "mail":{
    "timestamp":"2017-08-05T00:40:02.012Z",
    "source":"Sender Name <sender@example.com>",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
```

```
    "headers":[
      {
        "name":"From",
        "value":"Sender Name <sender@example.com>"
      },
      {
        "name":"To",
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Message sent from Amazon SES"
      },
      {
        "name":"MIME-Version",
        "value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"multipart/alternative; boundary=\"----
=_Part_7307378_1629847660.1516840721503\""
      }
    ],
    "commonHeaders":{
      "from":[
        "Sender Name <sender@example.com>"
      ],
      "to":[
        "recipient@example.com"
      ],
      "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject":"Message sent from Amazon SES"
    },
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ],
      "ses:source-ip":[
        "192.0.2.0"
      ],
      "ses:from-domain":[
        "example.com"
      ],
      "ses:caller-identity":[
```

```
        "ses_user"
      ]
    }
  }
}
```

Complaint-Datensatz

Im Folgenden finden Sie ein Beispiel für einen `Complaint` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType":"Complaint",
  "complaint": {
    "complainedRecipients":[
      {
        "emailAddress":"recipient@example.com"
      }
    ],
    "timestamp":"2017-08-05T00:41:02.669Z",
    "feedbackId":"01000157c44f053b-61b59c11-9236-11e6-8f96-7be8aexample-000000",
    "userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/60.0.3112.90 Safari/537.36",
    "complaintFeedbackType":"abuse",
    "arrivalDate":"2017-08-05T00:41:02.669Z"
  },
  "mail":{
    "timestamp":"2017-08-05T00:40:01.123Z",
    "source":"Sender Name <sender@example.com>",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"From",
        "value":"Sender Name <sender@example.com>"
      },
      {
        "name":"To",
```

```
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Message sent from Amazon SES"
      },
      {
        "name":"MIME-Version","value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"multipart/alternative; boundary=\"----
=_Part_7298998_679725522.1516840859643\""
      }
    ],
    "commonHeaders":{
      "from":[
        "Sender Name <sender@example.com>"
      ],
      "to":[
        "recipient@example.com"
      ],
      "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject":"Message sent from Amazon SES"
    },
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ],
      "ses:source-ip":[
        "192.0.2.0"
      ],
      "ses:from-domain":[
        "example.com"
      ],
      "ses:caller-identity":[
        "ses_user"
      ]
    }
  }
}
```

Delivery-Datensatz

Im Folgenden finden Sie ein Beispiel für einen `Delivery` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.


```
{
  "eventType": "Delivery",
  "mail": {
    "timestamp": "2016-10-19T23:20:52.240Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
```

```
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:outgoing-ip": [
        "192.0.2.0"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "delivery": {
    "timestamp": "2016-10-19T23:21:04.133Z",
    "processingTimeMillis": 11893,
    "recipients": [
      "recipient@example.com"
    ],
    "smtpResponse": "250 2.6.0 Message received",
    "remoteMtaIp": "123.456.789.012",
    "reportingMTA": "mta.example.com"
  }
```

```
}
```

Send-Datensatz

Im Folgenden finden Sie ein Beispiel für einen `Send` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType": "Send",
  "mail": {
    "timestamp": "2016-10-14T05:02:16.645Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/mixed;  boundary=\"----=_Part_0_716996660.1476421336341\""
      },
      {
        "name": "X-SES-MESSAGE-TAGS",
        "value": "myCustomTag1=myCustomTagValue1, myCustomTag2=myCustomTagValue2"
```

```
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "send": {}
}
```

Reject-Datensatz

Im Folgenden finden Sie ein Beispiel für einen `Reject` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType": "Reject",
```

```
  "mail": {
    "timestamp": "2016-10-14T17:38:15.211Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "sender@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/mixed; boundary=\"qMm9M+Fa2AknHoGS\""
      },
      {
        "name": "X-SES-MESSAGE-TAGS",
        "value": "myCustomTag1=myCustomTagValue1, myCustomTag2=myCustomTagValue2"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
```

```
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "reject": {
    "reason": "Bad content"
  }
}
```

Open-Datensatz

Im Folgenden finden Sie ein Beispiel für einen Open Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType": "Open",
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
```

```
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
```

```
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "IAM_user_or_role_name"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T21:59:49.927Z"
  },
  "open": {
    "ipAddress": "192.0.2.1",
    "timestamp": "2017-08-09T22:00:19.652Z",
    "userAgent": "Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X)
 AppleWebKit/603.3.8 (KHTML, like Gecko) Mobile/14G60"
  }
}
```

Click-Datensatz

Im Folgenden finden Sie ein Beispiel für einen `Click` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType": "Click",
  "click": {
    "ipAddress": "192.0.2.1",
    "link": "http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-
smtp.html",
    "linkTags": {
      "samplekey0": [
        "samplevalue0"
      ],
      "samplekey1": [
        "samplevalue1"
```

```
      ]
    },
    "timestamp": "2017-08-09T23:51:25.570Z",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/60.0.3112.90 Safari/537.36"
  },
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
```

```
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      },
      {
        "name": "Message-ID",
        "value": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000"
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T23:50:05.795Z"
  }
}
```

Rendering Failure-Datensatz

Im Folgenden finden Sie ein Beispiel für einen `Rendering Failure` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType":"Rendering Failure",
  "mail":{
    "timestamp":"2018-01-22T18:43:06.197Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "failure":{
    "errorMessage":"Attribute 'attributeName' is not present in the rendering data.",
    "templateName":"MyTemplate"
  }
}
```

DeliveryDelay aufzeichnen

Im Folgenden finden Sie ein Beispiel für einen `DeliveryDelay` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType": "DeliveryDelay",
  "mail":{
    "timestamp":"2020-06-16T00:15:40.641Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
```

```
        "ConfigSet"
      ]
    }
  },
  "deliveryDelay": {
    "timestamp": "2020-06-16T00:25:40.095Z",
    "delayType": "TransientCommunicationFailure",
    "expirationTime": "2020-06-16T00:25:40.914Z",
    "delayedRecipients": [{
      "emailAddress": "recipient@example.com",
      "status": "4.4.1",
      "diagnosticCode": "smtp; 421 4.4.1 Unable to connect to remote host"
    }]
  }
}
```

Abonnementdatensatz

Im Folgenden finden Sie ein Beispiel für einen `Subscription` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType": "Subscription",
  "mail": {
    "timestamp": "2022-01-12T01:00:14.340Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
    "destination": ["recipient@example.com"],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
```

```
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": ["sender@example.com"],
      "to": ["recipient@example.com"],
      "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:operation": ["SendEmail"],
      "ses:configuration-set": ["ConfigSet"],
      "ses:source-ip": ["192.0.2.0"],
      "ses:from-domain": ["example.com"],
      "ses:caller-identity": ["ses_user"],
      "myCustomTag1": ["myCustomValue1"],
      "myCustomTag2": ["myCustomValue2"]
    }
  },
  "subscription": {
    "contactList": "ContactListName",
    "timestamp": "2022-01-12T01:00:17.910Z",
    "source": "UnsubscribeHeader",
    "newTopicPreferences": {
      "unsubscribeAll": true,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    },
    "oldTopicPreferences": {
```

```
      "unsubscribeAll": false,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    }
  }
}
```

Interpretieren von Amazon SES-Ereignisdaten aus Amazon SNS

Amazon SES veröffentlicht E-Mail-Sendeereignisse für Amazon Simple Notification Service (Amazon SNS) als JSON-Datensätze. Amazon SNS stellt dann Benachrichtigungen an die Endpunkte zu, die das Amazon SNS-Thema im Zusammenhang mit dem Ereignisziel abonniert haben. Weitere Informationen zum Erstellen und Abonnieren eines Amazon-SNS-Themas finden Sie unter Erste Schritte mit Amazon SNS im Entwicklerhandbuch zu Amazon Simple Notification Service.

Eine Beschreibung der Datensatzinhalte und Beispieldatensätze finden Sie in den folgenden Abschnitten.

- Inhalte von Ereignisdatensätzen
- Beispiele für Ereignisdatensätze

Inhalt der Ereignisdaten, die Amazon SES in Amazon SNS veröffentlicht hat

Amazon SES veröffentlicht E-Mail-Sendeereignisdatensätze für Amazon Simple Notification Service im JSON-Format.

Beispieldatensätze für all diese Benachrichtigungstypen finden Sie unter Beispiele für Ereignisdaten, die Amazon SES in Amazon SNS veröffentlicht hat.

Themen in diesem Abschnitt:

- JSON-Objekt der obersten Ebene
- Mail-Objekt
- Bounce-Objekt
- Complaint-Objekt
- Delivery-Objekt

- Send-Objekt
- Reject-Objekt
- Open-Objekt
- Click-Objekt
- Rendering-Failure-Objekt
- DeliveryDelay Objekt
- Abonnementobjekt

JSON-Objekt der obersten Ebene

Das JSON-Objekt der obersten Ebene in einem E-Mail-Sendeereignisdatensatz enthält die folgenden Felder. Der Ereignistyp bestimmt, welche anderen Objekte vorhanden sind.

Feldname	Description
`eventType`	Eine Zeichenfolge, die die Art des Ereignisses angibt. Mögliche Werte: `Bounce`, `Complaint`, `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure`, `DeliveryDelay` oder `Subscription`. Wenn Sie keine Ereignisveröffentlichung einrichten heißt dieses Feld `notificationType`.
`mail`	Ein JSON-Objekt, das Informationen über die E-Mail enthält, die das Ereignis hervorgerufen hat.
`bounce`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Bounce` eingestellt ist. Es enthält Informationen über die Unzustellbarkeit.
`complaint`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Complaint` eingestellt ist. Es enthält Informationen über die Beschwerde.

Feldname	Description
`delivery`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Delivery` eingestellt ist. Es enthält Informationen über die Zustellung.
`send`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Send` eingestellt ist.
`reject`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Reject` eingestellt ist. Es enthält Informationen über die Ablehnung.
`open`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Open` eingestellt ist. Es enthält Informationen über das offene Ereignis.
`click`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Click` eingestellt ist. Es enthält Informationen über das Klick-Ereignis.
`failure`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Rendering Failure` eingestellt ist. Es enthält Informationen über das Rendering-Fehlerereignis.
`deliveryDelay`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `DeliveryDelay` eingestellt ist. Es enthält Informationen zur verzögerten Zustellung einer E-Mail.
`subscription`	Dieses Feld ist nur vorhanden, wenn `eventType` auf `Subscription` eingestellt ist. Es enthält Informationen zu den Abonnementeinstellungen.

Mail-Objekt

Jeder E-Mail-Sendeereignisprotokolleintrag enthält Informationen über die ursprüngliche E-Mail im `mail`-Objekt. Das JSON-Objekt enthält Informationen über ein `mail`-Objekt mit den folgenden Feldern.

Feldname	Description
`timestamp`	Datum und Uhrzeit im ISO8601 Format (YYYY-MM DDThh -:mm:ss.sz), an dem die Nachricht gesendet wurde.
`messageId`	Eine eindeutige ID, die Amazon SES der Nachricht zugewiesen hat. Amazon SES gibt diesen Wert an Sie zurück, wenn Sie die Nachricht gesendet haben. **Note** Diese Nachrichten-ID wurde von Amazon SES zugewiesen. Sie finden diese Mitteilungs-ID in der ursprüngl ichen E-Mail in den Feldern `headers` und `commonHeaders` des Objekts `mail`.
`source`	Die E-Mail-Adresse, von der die Nachricht gesendet wurde (die Envelope-MAIL-FROM-Adresse).
`sourceArn`	Der Amazon-Ressourcenname (ARN) der Identität, die zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt `sourceArn` den ARN der ID an, die – gemäß Autorisierung durch den Identitätsbesitzer – vom stellvertretenden Sender zum Senden der E-Mail verwendet werden soll. Weitere

Feldname	Description
	Informationen zur Sendeautorisierung finden Sie unter E-Mail-Authentifizierungsmethoden.
`sendingAccountId`	Die AWS Konto-ID des Kontos, das zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt `sendingAccountId` die Konto-ID des stellvertretenden Senders an.
`destination`	Eine Liste der E-Mail-Adressen, an die die ursprüngliche E-Mail gesendet wurde.
`headersTruncated`	Eine Zeichenfolge, die angibt, ob die Header in der Benachrichtigung abgeschnitten sind. Dies passiert, wenn die Header größer als 10 KB sind. Mögliche Werte sind `true` und `false`.
`headers`	Eine Liste der ursprünglichen Header der E-Mail. Jeder Header in der Liste verfügt über die Felder `name` und `value`. **Note** Jede Nachrichten-ID im Feld `headers` stammt von der ursprünglichen Nachricht, die Sie an Amazon SES übergeben haben. Die Nachrichten-ID, die Amazon SES der Nachricht später zugewiesen hat, befindet sich im Feld `messageId` des Objekts `mail`.

Feldname	Description
`commonHeaders`	Eine Zuordnung der ursprünglichen, häufig verwendeten Header der E-Mail. **Note** Die Nachrichten-ID im Feld `commonHeaders` ist die Nachrichten-ID, die Amazon SES der Nachricht später im Feld `messageId` des Objekts `mail` zugewiesen hat.
`tags`	Eine Liste von Tags, die der E-Mail-Adresse zugeordnet sind.

Bounce-Objekt

Das JSON-Objekt enthält Informationen über ein `Bounce`-Ereignis mit den folgenden Feldern.

Feldname	Description
`bounceType`	Der Unzustellbarkeitstyp, wie er von Amazon SES festgelegt wurde.
`bounceSubType`	Der untergeordnete Typ der Unzustellbarkeit, wie er von Amazon SES festgelegt wurde.
`bouncedRecipients`	Eine Liste mit Informationen über die Empfänger der ursprünglichen E-Mail, an die diese nicht zugestellt werden konnte.
`timestamp`	Datum und Uhrzeit im ISO8601 Format (YYYY-MM-:mm:ss.sz DDThh), an dem der ISP die Bounce-Benachrichtigung gesendet hat.
`feedbackId`	Eine eindeutige ID für die Unzustellbarkeit.

Feldname	Description
`reportingMTA`	Der Wert des `Reporting-MTA` -Felds der DSN. Dies ist der Wert der Message Transfer Authority (MTA), die versucht hat, die Zustellungs-, Weiterleitungs- oder Gateway-Operation durchzuführen, die in der DSN beschrieben ist. **Note** Dieses Feld wird nur dann angezeigt, wenn eine Zustellungsstatusbenachrichtigung (Delivery Status Notification, DNS) an die Unzustellbarkeitsbenachrichtigung angehängt wurde.

Empfänger, an die nicht zugestellt werden konnte

Ein Unzustellbarkeitsereignis kann für einen einzelnen Empfänger oder für mehrere Empfänger gelten. Das `bouncedRecipients`-Feld enthält eine Liste von Objekten – eines pro Empfänger, dessen E-Mail-Adresse ein Unzustellbarkeitsereignis hervorgerufen hat – und weist zusätzlich das folgende Feld auf.

Feldname	Description
`emailAddress`	Die E-Mail-Adresse des Empfängers. Ist eine DSN verfügbar, ist dies der Wert des `Final-Recipient` -Felds der DSN.

Wurde eine DSN an eine Unzustellbarkeitsbenachrichtigung angehängt, sind möglicherweise folgende Felder ebenfalls vorhanden.

Feldname	Description
`action`	Der Wert des `Action`-Felds der DSN. Es zeigt die Aktion an, die von der berichtenden MTA als Reaktion auf die gescheiterte Zustellung der Benachrichtigung an diesen Empfänger ausgeführt wurde.
`status`	Der Wert des `Status`-Felds der DSN. Dies ist der vom Transport unabhängige Statuscode pro Empfänger, der den Zustellstatus der Nachricht anzeigt.
`diagnosticCode`	Der vom berichtenden MTA gemeldete Statuscode. Dies ist der Wert des `Diagnostic-Code` -Felds der DSN. Dieses Feld ist möglicherweise nicht im DSN und daher auch nicht in JSON enthalten.

Unzustellbarkeitstypen

Jedes Unzustellbarkeitsereignis lässt sich einem der Typen zuordnen, die in der folgenden Tabelle aufgeführt sind.

Das System zur Ereignisveröffentlichung veröffentlicht nur permanente Unzustellbarkeiten und temporäre Unzustellbarkeiten, die nicht mehr von Amazon SES abgerufen werden. Wenn Sie Unzustellbarkeitsnachrichten erhalten, die mit `Permanent` gekennzeichnet sind, sollten Sie die entsprechenden E-Mail-Adressen aus Ihrer Mailingliste entfernen; Sie werden in Zukunft nicht mehr an sie senden können. `Transient`-Unzustellbarkeitsnachrichten werden an Sie gesendet, wenn eine Nachricht mehrmals temporär unzustellbar war und Amazon SES nicht mehr versucht, sie erneut zu senden. Es ist möglich, dass das erneute Senden einer E-Mail an eine Adresse später erfolgreich ist, die ursprünglich zu einem `Transient`-Bounce führte.

bounceType	bounceSubType	Description
`Undetermined`	`Undetermined`	Amazon SES konnte keinen bestimmten Grund für das Scheitern der Zustellung finden.

bounceType	bounceSubType	Description
`Permanent`	`General`	Amazon SES hat eine allgemeine permanente Unzustellbarkeit erhalten. Wenn Sie diese Art von Unzustellbarkeit erhalten, sollten Sie die E-Mail-Adresse des Empfängers aus Ihrer Mailing-Liste entfernen.
`Permanent`	`NoEmail`	Amazon SES hat eine Benachrichtigung über eine permanente Unzustellbarkeit enthalten, da die Ziel-E-Mail-Adresse nicht existiert. Wenn Sie diese Art von Unzustellbarkeit erhalten, sollten Sie die E-Mail-Adresse des Empfängers aus Ihrer Mailing-Liste entfernen.
`Permanent`	`Suppressed`	Amazon SES hat das Senden an diese Adresse unterdrückt, da bereits mehrere Zustellversuche aufgrund einer ungültigen Adresse fehlgeschlagen sind. Informationen zum Überschreiben der globalen Unterdrückungsliste finden Sie unterVerwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole.
`Permanent`	`OnAccountSuppressionList`	Amazon SES hat das Senden an diese Adresse unterdrückt, da sie sich auf der Unterdrückungsliste auf Kontoebene befindet. Dies zählt nicht für Ihre Unzustellbarkeitsraten-Metrik.
`Transient`	`General`	Amazon SES hat eine allgemeine Unzustellbarkeitsbenachrichtigung erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger zukünftig möglich.

bounceType	bounceSubType	Description
`Transient`	`MailboxFull`	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung erhalten, weil das Postfach voll ist. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger zukünftig möglich.
`Transient`	`MessageTooLarge`	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung aufgrund einer zu großen E-Mail erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie die Größe der Nachricht reduzieren.
`Transient`	`CustomTimeoutExceeded`	Amazon SES war nicht in der Lage, die E-Mail innerhalb der vom E-Mail-Absender angegebenen Zeit erfolgreich zuzustellen. (In der Bounce-Nachricht wird der Grund für mögliche fehlgeschlagene Zustellungsversuche innerhalb der definierten TTL angegeben.)
`Transient`	`ContentRejected`	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung aufgrund eines abgelehnten Inhalts erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie den Inhalt der Nachricht ändern.
`Transient`	`AttachmentRejected`	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung aufgrund eines abgelehnten Anhangs erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie den Anhang entfernen oder ändern.

Complaint-Objekt

Das JSON-Objekt enthält Informationen über ein `Complaint`-Ereignis mit den folgenden Feldern.

Feldname	Description
`complainedRecipients`	Eine Liste mit Informationen zu Empfängern, die sich möglicherweise beschwert haben.
`timestamp`	Datum und Uhrzeit im ISO8601 Format (YYYY-MM DDThh -:mm:ss.sz), an dem der ISP die Beschwerdebenachrichtigung gesendet hat.
`feedbackId`	Eine eindeutige ID für die Beschwerde.
`complaintSubType`	Der Untertyp der Beschwerde, wie von Amazon SES festgelegt.

Ist zudem ein Feedback-Bericht an die Beschwerde angehängt, sind möglicherweise die folgenden Felder vorhanden.

Feldname	Description
`userAgent`	Der Wert des `User-Agent` -Felds aus dem Feedback-Bericht. Gibt den Namen und die Version des Systems an, das den Bericht generiert hat.
`complaintFeedbackType`	Der Wert des `Feedback-Type` -Felds aus dem Feedback-Bericht, der vom ISP empfangen wurde. Enthält die Art des Feedbacks.
`arrivalDate`	Der Wert des *`Received-Date`* Felds *`Arrival-Date`* oder aus dem Feedback-Bericht im Format (YYYY-MM-:mm:ss.sz). ISO8601 DDThh Dieses Feld ist möglicher

Feldname	Description
	weise nicht im Bericht und daher auch nicht in JSON enthalten.

Empfänger, die sich beschwert haben

Das `complainedRecipients`-Feld enthält eine Liste von Empfängern, die sich möglicherweise beschwert haben.

> **Important**
>
> In den meisten Fällen ISPs werden die E-Mail-Adressen von Empfängern, die Beschwerden einreichen, geschwärzt. Aus diesem Grund enthält das Feld `complainedRecipients` eine Liste aller Personen, denen eine E-Mail zugesendet wurde, deren Adresse zu der Domäne gehört, die die Beschwerdebenachrichtigung ausgegeben hat.

JSON-Objekte in dieser Liste enthalten das folgende Feld.

Feldname	Description
`emailAddress`	Die E-Mail-Adresse des Empfängers.

Beschwerdetypen

Sie sehen möglicherweise die folgenden Beschwerdetypen im `complaintFeedbackType`-Feld, so wie sie vom meldenden ISP entsprechend der Website zu Internet Assigned Numbers Authority zugewiesen wurden:

Feldname	Description
`abuse`	Weist auf unerwünschte E-Mails oder eine andere Art von E-Mail-Missbrauch hin.
`auth-failure`	Bericht über einen E-Mail-Authentifizierungsfehler.

Feldname	Description
`fraud`	Weist auf einen Betrug oder Phishing hin.
`not-spam`	Weist darauf hin, dass die Entität, die den Bericht bereitstellt, die Nachricht nicht als Spam betrachtet. Dies kann verwendet werden, um eine Nachricht zu korrigieren, die fälschlic herweise als Spam gekennzeichnet oder kategorisiert wurde.
`other`	Gibt eine andere Art von Feedback an, das nicht zu den registrierten Typen passt.
`virus`	Meldet, dass in der ursprünglichen Nachricht ein Virus entdeckt wurde.

Beschwerde-Untertypen

Der Wert des Feldes `complaintSubType` kann entweder null oder `OnAccountSuppressionList` sein. Wenn der Wert `OnAccountSuppressionList` lautet, hat Amazon SES die Nachricht akzeptiert, aber nicht versucht, sie zu senden, da sie sich auf der Unterdrückungsliste auf Kontoebene befand.

Delivery-Objekt

Das JSON-Objekt enthält Informationen über ein `Delivery`-Ereignis mit den folgenden Feldern.

Feldname	Description
`timestamp`	Datum und Uhrzeit der Zustellung der E-Mail an den E-Mail-Server des Empfängers durch Amazon SES im ISO8601 Format (YYYY-MM-: mm:ss.sz). DDThh
`processingTimeMillis`	Die Zeit in Millisekunden zwischen dem Zeitpunkt, als Amazon SES die Anforderu ng des Senders angenommen hat, und dem

Feldname	Description
	Zeitpunkt, als die Nachricht an den Mail-Server des Empfängers übergeben hat.
`recipients`	Eine Liste der beabsichtigten Empfänger, für die das Übermittlungsereignis gilt.
`smtpResponse`	Die SMTP-Antwort des Remote-ISPs, der die E-Mail von Amazon SES zugelassen hat. Diese Nachricht variiert je nach E-Mail, empfangen dem Mail-Server und empfangendem ISP.
`reportingMTA`	Der Hostname des Amazon SES-Mail-Servers, der die E-Mail gesendet hat.
`remoteMtaIp`	Die IP-Adresse der MTA, an die Amazon SES die E-Mail zugestellt hat.

Send-Objekt

Das JSON-Objekt mit Informationen über das `send`-Ereignis ist immer leer.

Reject-Objekt

Das JSON-Objekt enthält Informationen über ein `Reject`-Ereignis mit den folgenden Feldern.

Feldname	Description
`reason`	Der Grund für die Ablehnung der E-Mail. Der einzige mögliche Wert ist `Bad content`. Er bedeutet, dass Amazon SES erkannt hat, dass die E-Mail einen Virus enthält. Wenn eine Nachricht abgelehnt wird, hält Amazon SES ihre Verarbeitung an und versucht nicht, sie dem E-Mail-Server des Empfängers zuzustell en.

Open-Objekt

Das JSON-Objekt enthält Informationen über ein `Open`-Ereignis mit den folgenden Feldern.

Feldname	Description
`ipAddress`	Die IP-Adresse des Empfängers.
`timestamp`	Datum und Uhrzeit des Auftretens des Öffnungsereignisses im Format (YYYY-MM-:mm:ss.sz). ISO8601 DDThh
`userAgent`	Der Benutzeragent des Geräts oder E-Mail-Client, mit dem der Empfänger die E-Mail geöffnet hat.

Click-Objekt

Das JSON-Objekt enthält Informationen über ein `Click`-Ereignis mit den folgenden Feldern.

Feldname	Description
`ipAddress`	Die IP-Adresse des Empfängers.
`timestamp`	Datum und Uhrzeit des Auftretens des Klickereignisses im Format (YYYY-MM-:mm:ss.sz). ISO8601 DDThh
`userAgent`	Der Benutzeragent des Clients, den der Empfänger zum Klicken auf einen Link in der E-Mail verwendet hat.
`link`	Die URL des Links, auf den der Empfänger geklickt hat.
`linkTags`	Eine Liste der Tags, die dem Link mithilfe des `ses:tags`-Attributs hinzugefügt wurden. Weitere Informationen zum Hinzufügen von Tags zu Links in Ihren E-Mails finden Sie unter

Feldname	Description
	F5. Kann ich Links mit eindeutigen Bezeichnern markieren? in den Amazon SES SES-Metriken zum Senden von E-Mails FAQs.

Rendering-Failure-Objekt

Das JSON-Objekt enthält Informationen über ein `Rendering Failure`-Ereignis mit den folgenden Feldern.

Feldname	Description
`templateName`	Der Name der Vorlage, die zum Senden der E-Mail verwendet wurde.
`errorMessage`	Eine Nachricht, die weitere Informationen über den Rendering-Fehler enthält.

DeliveryDelay Objekt

Das JSON-Objekt enthält Informationen über ein `DeliveryDelay`-Ereignis mit den folgenden Feldern.

Feldname	Description
`delayType`	Die Art der Verzögerung. Die möglichen Werte sind: • InternalFailure— Ein internes Amazon SES SES-Problem führte zu einer Verzögerung der Nachricht. • General – ein generischer Fehler ist während der SMTP-Konversation aufgetreten. • MailboxFull— Das Postfach des Empfängers ist voll und kann keine weiteren Nachrichten empfangen.

Feldname	Description
	• SpamDetected— Der E-Mail-Server des Empfängers hat eine große Menge unerwünschter E-Mails von Ihrem Konto erkannt. • RecipientServerError— Ein vorüberge hendes Problem mit dem E-Mail-Server des Empfängers verhindert die Zustellung der Nachricht. • IPFailure— Die IP-Adresse, über die die Nachricht gesendet wird, wird vom E-Mail-Anbieter des Empfängers blockiert oder gedrosselt. • TransientCommunicationFailure— Während der SMTP-Konversation mit dem E-Mail-Anbieter des Empfängers ist ein vorüberge hender Kommunikationsfehler aufgetreten. • BYOIPHostNameLookupUnavailable— Amazon SES konnte den DNS-Hostnamen für Ihre IP-Adressen nicht ermitteln. Diese Art von Verzögerung tritt nur auf, wenn Sie Bring Your Own IP verwenden. • Unbestimmt – Amazon SES konnte den Grund für die Lieferverzögerung nicht ermitteln. • SendingDeferral— Amazon SES hat es für angemessen erachtet, die Nachricht intern zu verschieben.
`delayedRecipients`	Ein Objekt, das Informationen zum E-Mail-Em pfänger enthält

Feldname	Description
`expirationTime`	Das Datum und die Uhrzeit, wann Amazon SES die Zustellung der Nachricht nicht mehr versucht. Dieser Wert wird im ISO 8601-Format angezeigt.
`reportingMTA`	Die IP-Adresse des Message Transfer Agent (MTA), der die Verzögerung gemeldet hat
`timestamp`	Datum und Uhrzeit, wann die Verzögerung aufgetreten ist (im ISO 8601-Format)

Empfänger, an die verzögert zugestellt wurde

Das `delayedRecipients`-Objekt enthält die folgenden Werte:

Feldname	Description
`emailAddress`	Die E-Mail-Adresse, die zu einer verzögerten Zustellung der Nachricht führte
`status`	Der SMTP-Statuscode, der der Zustellve rzögerung zugeordnet ist
`diagnosticCode`	Der Diagnosecode, der vom empfangenden Message Transfer Agent (MTA) bereitgestellt wird

Abonnementobjekt

Das JSON-Objekt enthält Informationen über ein `Subscription`-Ereignis mit den folgenden Feldern.

Feldname	Description
`contactList`	Der Name der Liste, auf der sich der Kontakt befindet.
`timestamp`	Datum und Uhrzeit im ISO8601 Format (YYYY-MM DDThh -:mm:ss.sz), an dem der ISP die Abonnementbenachrichtigung gesendet hat.
`source`	Die E-Mail-Adresse, von der die Nachricht gesendet wurde (die Envelope-MAIL-FROM-Adresse).
`newTopicPreferences`	Eine JSON-Datenstruktur (Zuweisung), die den Abonnementstatus aller Themen in der Kontaktliste angibt, die den Status nach einer Änderung (Kontakt abonniert oder Abonnement abbestellt) anzeigt.
`oldTopicPreferences`	Eine JSON-Datenstruktur (Zuweisung), die den Abonnementstatus aller Themen in der Kontaktliste angibt, die den Status vor der Änderung (Kontakt abonniert oder Abonnement abbestellt) anzeigt.

Einstellungen für neue/alte Themen

Die Objekte `newTopicPreferences` und `oldTopicPreferences` enthalten die folgenden Werte.

Feldname	Description
`unsubscribeAll`	Gibt an, ob der Kontakt das Abonnement von allen Themen in der Kontaktliste abbestellt hat.
`topicSubscriptionStatus`	Gibt den Abonnementstatus des Themas in dem `topicName` Feld an, das angibt, ob es derzeit für den Empfang von Benachric htigungen von SES für den angegebenen

Feldname	Description
	Ereignistyp angemeldet ist. Mögliche Werte sind OptIn(abonniert) oder OptOut(abgemeldet) in dem Feld. `subscriptionStatus`
`topicDefaultSubscriptionStatus`	Gibt den Standard-Abonnementstatus des Themas im `topicName` Feld an, der bestimmt, ob neue Themen, die dem Veranstaltungsziel hinzugefügt werden, standardmäßig abonniert oder abgemeldet werden. Mögliche Werte sind OptIn(standardmäßig abonniert) oder OptOut(standardmäßig abgemeldet) in dem Feld. `subscriptionStatus`

Beispiele für Ereignisdaten, die Amazon SES in Amazon SNS veröffentlicht hat

In diesem Abschnitt finden Sie Beispiele für die Typen von E-Mail-Sendeereignisdatensätzen, die Amazon SES für Amazon SNS veröffentlicht.

Themen in diesem Abschnitt:

- Bounce-Datensatz
- Complaint-Datensatz
- Delivery-Datensatz
- Send-Datensatz
- Reject-Datensatz
- Open-Datensatz
- Click-Datensatz
- Rendering Failure-Datensatz
- DeliveryDelay Rekord
- Abonnementdatensatz

> **Note**
>
> In den folgenden Beispielen wird, wenn ein `tag`-Feld verwendet wird, Ereignisveröffentlichung durch einen Konfigurationssatz verwendet, für den SES die Veröffentlichung von Tags für alle Ereignistypen unterstützt. Wenn Sie Feedback-Benachrichtigungen direkt über die Identität verwenden, veröffentlicht SES keine Tags. Lesen Sie mehr über das Hinzufügen von Tags, wenn Sie einen Konfigurationssatz erstellen oder einen Konfigurationssatz ändern.

Bounce-Datensatz

Nachfolgend finden Sie ein Beispiel eines `Bounce`-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht.

```
{
  "eventType":"Bounce",
  "bounce":{
    "bounceType":"Permanent",
    "bounceSubType":"General",
    "bouncedRecipients":[
      {
        "emailAddress":"recipient@example.com",
        "action":"failed",
        "status":"5.1.1",
        "diagnosticCode":"smtp; 550 5.1.1 user unknown"
      }
    ],
    "timestamp":"2017-08-05T00:41:02.669Z",
    "feedbackId":"01000157c44f053b-61b59c11-9236-11e6-8f96-7be8aexample-000000",
    "reportingMTA":"dsn; mta.example.com"
  },
  "mail":{
    "timestamp":"2017-08-05T00:40:02.012Z",
    "source":"Sender Name <sender@example.com>",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
```

```
    "headers":[
      {
        "name":"From",
        "value":"Sender Name <sender@example.com>"
      },
      {
        "name":"To",
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Message sent from Amazon SES"
      },
      {
        "name":"MIME-Version",
        "value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"multipart/alternative; boundary=\"----
=_Part_7307378_1629847660.1516840721503\""
      }
    ],
    "commonHeaders":{
      "from":[
        "Sender Name <sender@example.com>"
      ],
      "to":[
        "recipient@example.com"
      ],
      "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject":"Message sent from Amazon SES"
    },
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ],
      "ses:source-ip":[
        "192.0.2.0"
      ],
      "ses:from-domain":[
        "example.com"
      ],
      "ses:caller-identity":[
```

```
        "ses_user"
      ]
    }
  }
}
```

Complaint-Datensatz

Nachfolgend finden Sie ein Beispiel eines `Complaint`-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht.

```
{
  "eventType":"Complaint",
  "complaint": {
    "complainedRecipients":[
      {
        "emailAddress":"recipient@example.com"
      }
    ],
    "timestamp":"2017-08-05T00:41:02.669Z",
    "feedbackId":"01000157c44f053b-61b59c11-9236-11e6-8f96-7be8aexample-000000",
    "userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/60.0.3112.90 Safari/537.36",
    "complaintFeedbackType":"abuse",
    "arrivalDate":"2017-08-05T00:41:02.669Z"
  },
  "mail":{
    "timestamp":"2017-08-05T00:40:01.123Z",
    "source":"Sender Name <sender@example.com>",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"From",
        "value":"Sender Name <sender@example.com>"
      },
      {
        "name":"To",
```

```
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Message sent from Amazon SES"
      },
      {
        "name":"MIME-Version","value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"multipart/alternative; boundary=\"----
=_Part_7298998_679725522.1516840859643\""
      }
    ],
    "commonHeaders":{
      "from":[
        "Sender Name <sender@example.com>"
      ],
      "to":[
        "recipient@example.com"
      ],
      "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject":"Message sent from Amazon SES"
    },
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ],
      "ses:source-ip":[
        "192.0.2.0"
      ],
      "ses:from-domain":[
        "example.com"
      ],
      "ses:caller-identity":[
        "ses_user"
      ]
    }
  }
}
```

Delivery-Datensatz

Nachfolgend finden Sie ein Beispiel eines `Delivery`-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht.


```
{
  "eventType": "Delivery",
  "mail": {
    "timestamp": "2016-10-19T23:20:52.240Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
```

```
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:outgoing-ip": [
        "192.0.2.0"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "delivery": {
    "timestamp": "2016-10-19T23:21:04.133Z",
    "processingTimeMillis": 11893,
    "recipients": [
      "recipient@example.com"
    ],
    "smtpResponse": "250 2.6.0 Message received",
    "remoteMtaIp": "123.456.789.012",
    "reportingMTA": "mta.example.com"
  }
```

```
}
```

Send-Datensatz

Nachfolgend finden Sie ein Beispiel eines Send-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht. Einige Felder sind nicht immer vorhanden. Bei einer E-Mail mit Vorlagen wird der Betreff beispielsweise später gerendert und in nachfolgende Ereignisse aufgenommen.

```
{
  "eventType": "Send",
  "mail": {
    "timestamp": "2016-10-14T05:02:16.645Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/mixed;  boundary=\"----=_Part_0_716996660.1476421336341\""
      },
      {
        "name": "X-SES-MESSAGE-TAGS",
```

```
        "value": "myCustomTag1=myCustomTagValue1, myCustomTag2=myCustomTagValue2"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "send": {}
}
```

Reject-Datensatz

Nachfolgend finden Sie ein Beispiel eines `Reject`-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht.

```
{
```

```
  "eventType": "Reject",
  "mail": {
    "timestamp": "2016-10-14T17:38:15.211Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "sender@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/mixed; boundary=\"qMm9M+Fa2AknHoGS\""
      },
      {
        "name": "X-SES-MESSAGE-TAGS",
        "value": "myCustomTag1=myCustomTagValue1, myCustomTag2=myCustomTagValue2"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
```

```
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "reject": {
    "reason": "Bad content"
  }
}
```

Open-Datensatz

Nachfolgend finden Sie ein Beispiel eines Open-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht.

```
{
  "eventType": "Open",
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
```

```
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
```

```
      ],
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "IAM_user_or_role_name"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T21:59:49.927Z"
  },
  "open": {
    "ipAddress": "192.0.2.1",
    "timestamp": "2017-08-09T22:00:19.652Z",
    "userAgent": "Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X)
 AppleWebKit/603.3.8 (KHTML, like Gecko) Mobile/14G60"
  }
}
```

Click-Datensatz

Nachfolgend finden Sie ein Beispiel eines `Click`-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht.

```
{
  "eventType": "Click",
  "click": {
    "ipAddress": "192.0.2.1",
    "link": "http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-
smtp.html",
    "linkTags": {
      "samplekey0": [
        "samplevalue0"
      ],
      "samplekey1": [
```

```
        "samplevalue1"
      ]
    },
    "timestamp": "2017-08-09T23:51:25.570Z",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/60.0.3112.90 Safari/537.36"
  },
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
```

```
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      },
      {
        "name": "Message-ID",
        "value": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000"
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T23:50:05.795Z"
  }
}
```


Rendering Failure-Datensatz

Nachfolgend finden Sie ein Beispiel eines `Rendering Failure`-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht.

```
{
  "eventType":"Rendering Failure",
  "mail":{
    "timestamp":"2018-01-22T18:43:06.197Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "failure":{
    "errorMessage":"Attribute 'attributeName' is not present in the rendering data.",
    "templateName":"MyTemplate"
  }
}
```

DeliveryDelay Rekord

Nachfolgend finden Sie ein Beispiel eines `DeliveryDelay`-Ereignisdatensatzes, den Amazon SES für Amazon SNS veröffentlicht.

```
{
  "eventType": "DeliveryDelay",
  "mail":{
    "timestamp":"2020-06-16T00:15:40.641Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
```

```
        "ConfigSet"
      ]
    }
  },
  "deliveryDelay": {
    "timestamp": "2020-06-16T00:25:40.095Z",
    "delayType": "TransientCommunicationFailure",
    "expirationTime": "2020-06-16T00:25:40.914Z",
    "delayedRecipients": [{
      "emailAddress": "recipient@example.com",
      "status": "4.4.1",
      "diagnosticCode": "smtp; 421 4.4.1 Unable to connect to remote host"
    }]
  }
}
```

Abonnementdatensatz

Im Folgenden finden Sie ein Beispiel für einen `Subscription` Ereignisdatensatz, den Amazon SES auf Firehose veröffentlicht.

```
{
  "eventType": "Subscription",
  "mail": {
    "timestamp": "2022-01-12T01:00:14.340Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
    "destination": ["recipient@example.com"],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
```

```
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": ["sender@example.com"],
      "to": ["recipient@example.com"],
      "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:operation": ["SendEmail"],
      "ses:configuration-set": ["ConfigSet"],
      "ses:source-ip": ["192.0.2.0"],
      "ses:from-domain": ["example.com"],
      "ses:caller-identity": ["ses_user"],
      "myCustomTag1": ["myCustomValue1"],
      "myCustomTag2": ["myCustomValue2"]
    }
  },
  "subscription": {
    "contactList": "ContactListName",
    "timestamp": "2022-01-12T01:00:17.910Z",
    "source": "UnsubscribeHeader",
    "newTopicPreferences": {
      "unsubscribeAll": true,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    },
    "oldTopicPreferences": {
```

```
      "unsubscribeAll": false,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    }
  }
}
```

Überwachen Ihrer Amazon SES-Absenderzuverlässigkeit

Amazon SES verfolgt aktiv mehrere Metriken, die Ihrer Zuverlässigkeit als Sender schaden oder dazu führen könnten, dass Ihre E-Mail-Zustellungsquoten zurückgehen. Zwei wichtige Metriken, die wir in diesem Prozess berücksichtigen, sind die Unzustellbarkeits- und Beschwerdequoten für Ihr Konto. Wenn die Unzustellbarkeits- oder Beschwerdequoten für Ihr Konto zu hoch sind, legen wir möglicherweise eine Prüfung für Ihr Konto fest oder unterbrechen die Fähigkeit Ihres Kontos zum Versenden von E-Mails.

Da Ihre Unzustellbarkeits- und Beschwerdequote so wichtig für den Zustand Ihres Kontos ist, enthält Amazon SES ein Zuverlässigkeits-Dashboard, auf dem Sie diese Metriken verfolgen können. Das Zuverlässigkeits-Dashboard kann auch Informationen zu Faktoren anzeigen, die nicht im Zusammenhang mit Unzustellbarkeiten oder Beschwerden stehen, die Ihrer Absenderzuverlässigkeit schaden könnten. Wenn Sie beispielsweise eine E-Mail an eine bekannte spamtrap senden, wird eine Meldung auf diesem Dashboard angezeigt.

Dieser Abschnitt enthält Informationen über den Zugriff auf das Zuverlässigkeits-Dashboard, die Interpretation der enthaltenen Informationen und die Einrichtung von Systemen, damit Sie aktiv über Faktoren informiert werden, die Auswirkungen auf Ihre Absenderzuverlässigkeit haben könnten.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Verwenden des Reputation Dashboards zum Nachverfolgen von Unzustellbarkeits- und Beschwerdequoten
- Reputation Metriken Nachrichten
- Erstellen von Alarmen zur Reputationsüberwachung mit CloudWatch
- SNDS-Metriken für dedizierte IPs
- Automatisches Unterbrechen des E-Mail-Versands

Verwenden des Reputation Dashboards zum Nachverfolgen von Unzustellbarkeits- und Beschwerdequoten

Das Reputation Dashboard enthält dieselben Informationen, die dem Amazon SES-Team bei der Überprüfung des Zustands einzelner Konten angezeigt werden.

So zeigen Sie Replikationsmetriken an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich auf der linken Seite des Bildschirms die Option Reputation Dashboard aus.

   Das Dashboard zeigt die folgenden Informationen an:

   - Konto-Status— Eine Zusammenfassung der kombinierten Gesundheit Ihrer Unzustellstellbaren und Beschwerdequoten. Mögliche Werte sind:
     - Healthy – Es gibt derzeit keine Probleme, die sich auf Ihr Konto auswirken.
     - Under review (Wird geprüft) – Ihr Konto wird geprüft. Wenn die Probleme, die dazu führten, dass wir eine Prüfung für Ihr Konto festgelegt haben, am Ende des Überprüfungszeitraums nicht behoben sind, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden.
     - Pending end of review decision (Entscheidung am Ende der Überprüfung ausstehend) – Ihr Konto wird geprüft. Aufgrund der Art der Probleme, die zur Festlegung einer Prüfung für Ihr Konto führten, müssen wir zunächst eine manuelle Prüfung Ihres Kontos durchführen, bevor wir weitere Maßnahmen ergreifen.
     - Sending paused (Senden angehalten) – Wir haben die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrochen. Während die Fähigkeit Ihres Konto zum Versenden von E-Mails unterbrochen ist, können Sie mit Amazon SES keine E-Mails senden. Sie können anfordern, dass wir diese Entscheidung überprüfen. Weitere Informationen zum Anfordern einer Überprüfung finden Sie unter Amazon SES Versandprüfungsprozess FAQs.
     - Pending sending pause (Sendeunterbrechung ausstehend) – Ihr Konto wird geprüft. Die Probleme, die dazu führten, dass wir eine Prüfung für Ihr Konto festgelegt haben, wurden nicht behoben. In diesem Fall unterbrechen wir gewöhnlich die Fähigkeit Ihres Kontos, E-Mails zu senden. Aufgrund der Art Ihres Kontos müssen wir zunächst Ihr Konto überprüfen, bevor weitere Maßnahmen ergriffen werden.
   - Bounce Rate – Der Prozentsatz der von Ihrem Konto gesendeten E-Mails, die dauerhaft unzustellbar waren. Siehe wie Ihre Unzustellbarkeitsrate berechnet wird.
   - Complaint Rate – Der Prozentsatz der von Ihrem Konto gesendeten E-Mails, die von Empfängern als Spam gemeldet wurden. Siehe wie Ihre Beschwerderate berechnet wird

> **Note**
>
> Die Abschnitte Bounce Rate und Complaint Rate enthalten außerdem Statusmeldungen zu den jeweiligen Metriken. In der folgenden Liste sind Statusmeldungen aufgeführt, die möglicherweise für diese Metriken angezeigt werden:
>
> - Healthy – Die Metrik befindet sich im Normalbereich.
> - Almost healed (Fast behoben) – Aufgrund der Metrik wurde eine Prüfung für Ihr Konto festgelegt. Seit Beginn des Überprüfungszeitraums blieb die Metrik unterhalb der Höchstrate. Wenn die Metrik unterhalb der Höchstrate bleibt, ändert sich der Status dieser Metrik vor Ablauf des Überprüfungszeitraums in Healthy (Stabil).
> - Under review (Wird geprüft) – Aufgrund der Metrik wurde eine Prüfung für Ihr Konto festgelegt und es befindet sich weiterhin oberhalb der Höchstrate. Wenn das Problem, das zu einer Überschreitung der Höchstrate der Metrik führte, bis zum Ablauf des Überprüfungszeitraums nicht behoben wurde, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden.
> - Sending pause (Sendeunterbrechung) – Aufgrund der Metrik haben wir die Fähigkeit Ihres Kontos unterbrochen, E-Mails zu senden. Solange die Fähigkeit Ihres Konto zum Versenden von E-Mails unterbrochen ist, können Sie mit Amazon SES keine E-Mails senden. Sie können anfordern, dass wir diese Entscheidung überprüfen. Weitere Informationen zum Senden einer Überprüfungsanfrage finden Sie unter Amazon SES Versandprüfungsprozess FAQs.
> - Pending sending pause – Aufgrund der Metrik haben wir eine Prüfung für Ihr Konto festgelegt. Die Probleme, die diesen Überprüfungszeitraum verursacht haben, sind nicht gelöst. Diese Probleme können uns möglicherweise dazu bewegen, die Fähigkeit des Kontos zum Senden von E-Mails zu unterbrechen. Ein Mitglied des Amazon SES-Teams muss Ihr Konto überprüfen, bevor wir weitere Maßnahmen ergreifen.

- Andere Benachrichtigungen – Wenn bei Ihrem Konto Probleme im Hinblick auf die Zuverlässigkeit auftreten, die aber nicht mit unzustellbaren Nachrichten oder Beschwerden im Zusammenhang stehen, wird hier eine kurze Nachricht angezeigt. Weitere Informationen über die Benachrichtigungen, die in diesem Bereich angezeigt werden können, finden Sie unter Reputation Metriken Nachrichten.

Reputation Metriken Nachrichten

Das Amazon SES Reputation Dashboard stellt wichtige Metriken zu Ihrem Konto zur Verfügung. In den folgenden Abschnitten werden die Nachrichten beschrieben, die im Dashboard angezeigt werden können. Zudem finden Sie hilfreiche Tipps und Informationen, mit denen Sie Probleme im Zusammenhang mit Ihrer Senderzuverlässigkeit möglicherweise beheben können.

In diesem Thema finden Sie Informationen zu den folgenden Benachrichtigungstypen:

- Statusnachrichten
- Benachrichtigung zur Unzustellbarkeitsquote
- Benachrichtigung zur Beschwerdequote
- Benachrichtigungen zur Anti-Spam-Organisation
- Listbombing-Benachrichtigung
- Benachrichtigungen zu direktem Feedback
- Domain-Blocklist-Benachrichtigungen
- Benachrichtigung zur internen Überprüfung
- Benachrichtigung zum E-Mail-Dienstanbieter
- Benachrichtigung zu Empfänger-Feedback
- Benachrichtigung zu verknüpftem Konto
- Benachrichtigung zu Pseudo-E-Mail-Adressen für Spam
- Benachrichtigung zur Websiteanfälligkeit
- Benachrichtigung zu kompromittierten Anmeldeinformationen
- Sonstige Benachrichtigung

Statusnachrichten

Wenn Sie das Reputation Dashboard verwenden, sehen Sie eine Nachricht, in welcher der Status Ihres Amazon-SES-Kontos beschrieben wird. Nachfolgend finden Sie eine Liste mit den möglichen Kontostatuswerten:

- Healthy – Es gibt derzeit keine Probleme, die sich auf Ihr Konto auswirken.

- Under review (Wird geprüft) – Ihr Konto wird geprüft. Wenn die Probleme, die dazu führten, dass wir eine Prüfung für Ihr Konto festgelegt haben, am Ende des Überprüfungszeitraums nicht behoben sind, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden.
- Pending end of review decision (Entscheidung am Ende der Überprüfung ausstehend) – Ihr Konto wird geprüft. Aufgrund der Art der Probleme, die zur Festlegung einer Prüfung für Ihr Konto führten, müssen wir zunächst eine manuelle Prüfung Ihres Kontos durchführen, bevor wir weitere Maßnahmen ergreifen.
- Sending paused (Senden angehalten) – Wir haben die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrochen. Während die Fähigkeit Ihres Konto zum Versenden von E-Mails unterbrochen ist, können Sie mit Amazon SES keine E-Mails senden. Sie können anfordern, dass wir diese Entscheidung überprüfen. Weitere Informationen zum Anfordern einer Überprüfung finden Sie unter Amazon SES Versandprüfungsprozess FAQs.
- Pending sending pause (Sendeunterbrechung ausstehend) – Ihr Konto wird geprüft. Die Probleme, die dazu führten, dass wir eine Prüfung für Ihr Konto festgelegt haben, wurden nicht behoben. In diesem Fall unterbrechen wir gewöhnlich die Fähigkeit Ihres Kontos, E-Mails zu senden. Aufgrund der Art Ihres Kontos müssen wir zunächst Ihr Konto überprüfen, bevor weitere Maßnahmen ergriffen werden.

Zudem werden in den Reputation Dashboard-Bereichen Bounce Rate und Complaint Rate Statusübersichten für die zugehörigen Metriken angegeben. Nachfolgend finden Sie eine Liste mit den möglichen Metrikstatuswerten:

- Healthy (Stabil) – Die Metrik befindet sich im Normalbereich.
- Almost healed (Fast behoben) – Aufgrund der Metrik wurde eine Prüfung für Ihr Konto festgelegt. Seit Beginn des Überprüfungszeitraums blieb die Metrik unterhalb der Höchstrate. Wenn die Metrik unterhalb der Höchstrate bleibt, ändert sich der Status dieser Metrik vor Ablauf des Überprüfungszeitraums in Healthy (Stabil).
- Under review (Wird geprüft) – Aufgrund der Metrik wurde eine Prüfung für Ihr Konto festgelegt und es befindet sich weiterhin oberhalb der Höchstrate. Wenn das Problem, das zu einer Überschreitung der Höchstrate der Metrik führte, bis zum Ablauf des Überprüfungszeitraums nicht behoben wurde, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden.
- Sending pause (Sendeunterbrechung) – Aufgrund der Metrik haben wir die Fähigkeit Ihres Kontos unterbrochen, E-Mails zu senden. Solange die Fähigkeit Ihres Konto zum Versenden von E-Mails unterbrochen ist, können Sie mit Amazon SES keine E-Mails senden. Sie können anfordern, dass

wir diese Entscheidung überprüfen. Weitere Informationen zum Senden einer Überprüfungsanfrage finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

- Pending sending pause – Aufgrund der Metrik haben wir eine Prüfung für Ihr Konto festgelegt. Die Probleme, die diesen Überprüfungszeitraum verursacht haben, sind nicht gelöst. Diese Probleme können uns möglicherweise dazu bewegen, die Fähigkeit des Kontos zum Senden von E-Mails zu unterbrechen. Ein Mitglied des Amazon-SES-Teams muss Ihr Konto überprüfen, bevor wir weitere Maßnahmen ergreifen.

Benachrichtigung zur Unzustellbarkeitsquote

In diesem Abschnitt finden Sie zusätzliche Informationen über die Benachrichtigungen zur Unzustellbarkeitsquote, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Sie haben diese Benachrichtigung erhalten, da die Unzustellbarkeitsquote für Ihr Konto zu hoch war. Die Unzustellbarkeitsquote basiert auf der Anzahl permanenter Unzustellbarkeiten, die von Ihrem Amazon-SES-Konto generiert wurden. Bei den meisten E-Mail-Anbietern gilt eine hohe Unzustellbarkeitsquote als Zeichen dafür, dass der Sender seine Empfängerliste nicht ordnungsgemäß verwaltet und möglicherweise sogar unerwünschte E-Mails sendet.

Eine permanente Unzustellbarkeit tritt auf, wenn eine E-Mail an eine Adresse gesendet wird, die nicht vorhanden ist. In dieser Berechnung werden temporäre Unzustellbarkeiten, die auftreten, wenn ein Empfänger Ihre Nachricht vorübergehend nicht erhalten kann, nicht von Amazon SES berücksichtigt. Unzustellbare E-Mails, die Sie an verifizierte Adressen und Domänen senden, sowie von Ihnen an den Amazon-SES-Postfachsimulator gesendete E-Mails werden ebenfalls nicht in diese Berechnung einbezogen.

Wir berechnen Ihre Unzustellbarkeitsquote basierend auf einem repräsentativen E-Mail-Volumen. Eine repräsentative Menge ist eine Anzahl von E-Mails, die Ihr typisches Sendeverhalten repräsentiert. Um sowohl Sendern großer Mengen als auch Sendern kleinerer Mengen gerecht zu werden, ist die repräsentative Menge für jedes Konto unterschiedlich und ändert sich, wenn sich das Sendemuster des Kontos ändert.

Sie erzielen die besten Ergebnisse mit einer Unzustellbarkeitsquote von unter 5 %. Höhere Unzustellbarkeitsquoten können den Versand Ihrer E-Mails beeinflussen. Wenn Ihre Unzustellbarkeitsquote mehr als 5 % beträgt, legen wir für Ihr Konto automatisch eine Prüfung fest. Wenn Ihre Unzustellbarkeitsquote 10 % oder höher ist, unterbrechen wir möglicherweise die

Fähigkeit Ihres Kontos zum Versenden weiterer E-Mails, bis Sie das Problem behoben haben, das zu der hohen Unzustellbarkeitsquote führte.

Wie können Sie das Problem beheben?

Sofern noch nicht geschehen, etablieren Sie einen Prozess zum Erfassen und Verwalten von Unzustellbarkeiten und Beschwerden. Solche Prozesse müssen für alle Amazon-SES-Konten vorhanden sein. Weitere Informationen finden Sie unter Erfolgsmetriken von E-Mail-Programmen.

Ermitteln Sie als Nächstes, welche E-Mail-Adressen unzustellbar sind, und erstellen und implementieren Sie einen Plan, um diese Unzustellbarkeiten zu reduzieren oder aufzuheben. Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, bereits unterbrochen wurde, melden Sie sich bei an AWS-Managementkonsole und gehen Sie zu. AWS Support Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben.

Wenn Ihr Konto geprüft wird

Falls die Unzustellbarkeitsquote für Ihr Konto am Ende des Überprüfungszeitraums weiterhin über 10 % liegt, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie dieses Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Beschreiben Sie in Ihrer Antwort auf den Fall die Änderungen, die Sie implementiert haben. Wenn wir Ihnen zustimmen, dass diese Änderungen Ihre Unzustellbarkeitsquote senken, werden die Berechnungen entsprechend angepasst und nur die nach der Änderungsumsetzung aufgetretenen Unzustellbarkeiten berücksichtigt.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vornehmen, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Benachrichtigung zur Beschwerdequote

In diesem Abschnitt finden Sie zusätzliche Informationen über die Benachrichtigungen zur Beschwerdequote, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Sie haben diese Benachrichtigung erhalten, da die Beschwerdequote für Ihr Konto zu hoch war. Die Beschwerdequote basiert auf der Anzahl der Beschwerden, die von Ihrem Amazon-SES-Konto generiert werden. Bei den meisten E-Mail-Anbietern gilt eine hohe Beschwerdequote als Zeichen dafür, dass der Sender seine Empfängerliste nicht ordnungsgemäß verwaltet und möglicherweise sogar unerwünschte E-Mails sendet.

Eine Beschwerde tritt auf, wenn ein Empfänger eine E-Mail identifiziert, die Sie als Spam gesendet haben. Dies tritt in der Regel auf, wenn der Empfänger die Schaltfläche zum Melden von Spam in seinem E-Mail-Client verwendet. Beschwerden, die durch E-Mail-Nachrichten generiert werden, die Sie an den Amazon-SES-Posteingangssimulator senden, werden in dieser Berechnung nicht berücksichtigt.

Wir berechnen Ihre Beschwerdequote basierend auf einem repräsentativen E-Mail-Volumen. Eine repräsentative Menge ist eine Anzahl von E-Mails, die Ihr typisches Sendeverhalten repräsentiert. Um sowohl Sendern großer Mengen als auch Sendern kleinerer Mengen gerecht zu werden, ist die repräsentative Menge für jedes Konto unterschiedlich und ändert sich, wenn sich das Sendemuster des Kontos ändert.

Sie erzielen die besten Ergebnisse mit einer Beschwerdequote von unter 0,1 %. Höhere Beschwerdequoten können den Versand Ihrer E-Mails beeinflussen. Wenn Ihre Beschwerdequote mehr als 0,1 % beträgt, legen wir für Ihr Konto automatisch eine Prüfung fest. Wenn Ihre Beschwerdequote 0,5 % oder höher ist, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos zum Versenden weiterer E-Mails, bis Sie das Problem behoben haben, das zu der hohen Beschwerdequote führte.

Wie können Sie das Problem beheben?

Sofern noch nicht geschehen, etablieren Sie einen Prozess zum Erfassen und Verwalten von Unzustellbarkeiten und Beschwerden. Solche Prozesse müssen für alle Amazon-SES-Konten vorhanden sein. Weitere Informationen finden Sie unter Erfolgsmetriken von E-Mail-Programmen.

Ermitteln Sie als Nächstes, welche der von Ihnen gesendeten E-Mails zu Beschwerden führen, und implementieren Sie einen Plan, um diese Beschwerden zu reduzieren. Wenn die Fähigkeit Ihres

Kontos, E-Mails zu senden, bereits unterbrochen wurde, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben.

Sie sollten sofort damit aufhören, E-Mails an Adressen zu senden, von denen Sie Beschwerden erhalten haben – aber Sie sollten unbedingt die Faktoren ermitteln, die bei den Empfängern zur Beschwerde geführt haben. Wenn Sie diese Faktoren identifiziert haben, korrigieren Sie das E-Mail-Sendeverhalten entsprechend.

Wenn Ihr Konto geprüft wird

Falls die Beschwerdequote für Ihr Konto am Ende des Überprüfungszeitraums weiterhin über 0,5 % liegt, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie dieses Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Beschreiben Sie in Ihrer Antwort auf den Fall die Änderungen, die Sie implementiert haben. Wenn wir Ihnen zustimmen, dass diese Änderungen Ihre Beschwerdequote senken, werden die Berechnungen entsprechend angepasst und nur die nach der Änderungsumsetzung aufgetretenen Beschwerden berücksichtigt.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Benachrichtigungen zur Anti-Spam-Organisation

In diesem Abschnitt finden Sie zusätzliche Informationen über die Benachrichtigungen zur Anti-Spam-Organisation, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Von einer namhaften Anti-Spam-Organisation wurde gemeldet, dass der über Ihr Amazon-SES-Konto gesendete Inhalt von deren Systemen teilweise als unerwünscht oder problematisch erkannt wurde.

Wir können keine Informationen zu bestimmten Nachrichten bereitstellen, die dazu geführt haben, dass die Anti-Spam-Organisation Ihre Inhalte als problematisch kennzeichnete. Wir können den Namen der Organisation, von der diese Meldung stammt, nicht angeben. In der Regel berücksichtigen Anti-Spam-Organisationen eine Kombination aus folgenden Faktoren: Rückmeldung der Empfänger, Nachrichteneinbindungsmetriken, Zustellungsversuche an ungültige Adressen, von den Spam-Filtern markierter Inhalt sowie Treffer bei Pseudo-E-Mail-Adressen für Spam. Dies ist keine vollständige Liste. Möglicherweise wurden diese Organisationen aufgrund von anderen Faktoren veranlasst, Ihren Inhalt als Spam zu klassifizieren.

Wie können Sie das Problem beheben?

Zur Behebung dieses Problems müssen Sie ermitteln, aufgrund welcher Aspekte Ihres E-Mail-Programms die Anti-Spam-Organisation Ihre E-Mail möglicherweise als problematisch einstuft. Anschließend müssen Sie das Programm entsprechend anpassen, um das Problem zu lösen.

Wenn Ihr Konto geprüft wird

Wenn die Anti-Spam-Organisation am Ende des Überprüfungszeitraums die von Ihrem Konto gesendete E-Mail weiterhin als problematisch einstuft, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie das Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Gehen Sie in Ihrer Nachricht detailliert auf die von Ihnen vorgenommenen Änderungen ein. Nach Erhalt dieser Nachricht verlängern wir den Überprüfungszeitraum, sodass wir nur die Benachrichtigungen zur Anti-Spam-Organisation analysieren, die nach der Implementierung Ihrer Änderungen eingegangen sind. Sofern Ihr Konto am Ende des verlängerten Überprüfungszeitraums nicht mehr von der Anti-Spam-Organisation gelistet wird, beenden wir den Überprüfungszeitraum für Ihr Konto.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Listbombing-Benachrichtigung

In diesem Abschnitt finden Sie zusätzliche Informationen über Listbombing-Benachrichtigungen, die im Amazon-SES-Reputation-Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Eine Anti-Spam-Organisation hat festgestellt, dass Ihre E-Mail-Sendeprozesse anfällig für „Listbombing“ sind. Listbombing ist eine Form des Missbrauchs, bei der ein Angreifer eine sehr große Anzahl von E-Mail-Adressen in einem webbasierten Formular registriert. Listbombing kann zu Serviceunterbrechungen für die Benutzer der betroffenen E-Mail-Services führen. Es kann auch dazu führen, dass Ihre E-Mail von E-Mail-Anbietern blockiert wird.

Anti-Spam-Organisationen verwenden proprietäre Methoden, um Websites zu identifizieren, die anfällig für Listbombing sind. Aus diesem Grund können wir keine zusätzlichen Informationen zu dem Problem bereitstellen, das die Anti-Spam-Organisation dazu veranlasst hat, Ihren E-Mail-Sendeprozess als problematisch zu identifizieren. Darüber hinaus dürfen wir den Namen der Organisation, die das Problem erkannt hat, nicht nennen.

Wie können Sie das Problem beheben?

Sie sollten alle Ihre webbasierten Anmeldeformulare überprüfen, um sicherzustellen, dass sie nicht anfällig für diese Art von Missbrauch sind. Jedes Formular sollte ein CAPTCHA enthalten, um zu verhindern, dass automatisierte Skripts Abonnementanfragen übermitteln. Senden Sie außerdem neuen Benutzern, die sich für Ihr Produkt oder Ihren Service anmelden, eine E-Mail zur Bestätigung, dass sie sich tatsächlich anmelden wollten. Senden Sie den Kunden nur dann weitere E-Mails, wenn sie dem Empfang Ihrer Mitteilungen ausdrücklich zugestimmt haben.

Außerdem sollten Sie eine Freigabeerlaubnis von Ihrer E-Mail-Liste einholen. Dabei senden Sie eine E-Mail an alle Ihre Kunden und fragen sie, ob sie weiterhin E-Mails von Ihnen erhalten möchten. Senden Sie E-Mails nur an Kunden, die bestätigen, dass sie weiterhin E-Mails von Ihnen erhalten möchten.

Wenn Ihr Konto geprüft wird

Wenn die Anti-Spam-Organisation am Ende des Überprüfungszeitraums die von Ihrem Konto gesendete E-Mail weiterhin als problematisch einstuft, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie das Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Gehen Sie in Ihrer Nachricht detailliert auf die von Ihnen vorgenommenen Änderungen ein. Nach Erhalt dieser Nachricht verlängern wir den Überprüfungszeitraum, sodass wir nur die Benachrichtigungen zur Anti-Spam-Organisation analysieren, die nach der Implementierung Ihrer Änderungen eingegangen sind. Sofern Ihr Konto am Ende des verlängerten Überprüfungszeitraums nicht mehr von der Anti-Spam-Organisation gelistet wird, beenden wir den Überprüfungszeitraum für Ihr Konto.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Benachrichtigungen zu direktem Feedback

In diesem Abschnitt finden Sie zusätzliche Informationen über Benachrichtigungen zu direktem Feedback, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Zahlreiche Benutzer wenden sich direkt an Amazon SES und melden Nachrichten, die sie von einer Adresse oder einer Domäne erhalten haben, die mit Ihrem Amazon-SES-Konto verknüpft ist. Diese Art von Feedback wird weder in den direkten Beschwerdeberichten der E-Mail-Anbieter noch in den Unzustellbarkeits- und Beschwerdemetriken im Reputation Dashboard erfasst.

Um den Datenschutz der Benutzer zu gewährleisten, die diese Probleme gemeldet haben, können wir deren E-Mail-Adressen nicht zur Verfügung stellen.

Empfänger beschweren sich möglicherweise bei Amazon SES, wenn sie Nachrichten erhalten, für die sie sich nicht angemeldet haben, wenn sie nicht den erwarteten E-Mail-Typ erhalten, wenn sie die erhaltenen Nachrichten nicht hilfreich oder interessant finden, wenn sie nicht mehr wissen, dass sie sich für diese Nachrichten angemeldet haben, oder wenn sie zu viele Nachrichten bekommen. Diese Liste ist nicht vollständig. Die für Sie relevanten Faktoren hängen von Ihrem jeweiligen E-Mail-Programm ab.

Wie können Sie das Problem beheben?

Es wird empfohlen, bei der Akquise neuer E-Mail-Adressen eine Strategie der doppelten Anmeldung einzusetzen, wie unter Erstellen und Pflegen von Listen beschrieben, und auch nur E-Mails an Adressen zu senden, die diese doppelte Anmeldung ausgeführt haben.

Des Weiteren sollten Sie Adressen aus Ihren Listen löschen, die in letzter Zeit nicht mehr mit Ihren E-Mails interagiert haben. Sie können mithilfe der Nachverfolgungsfunktion für Öffnen und Klicken ermitteln, welche Benutzer die von Ihnen gesendeten Inhalte ansehen und damit interagieren, wie unter Überwachen Ihrer Amazon SES-Sendeaktivität beschrieben.

Wenn Ihr Konto geprüft wird

Wenn Amazon SES am Ende des Überprüfungszeitraums weiterhin eine signifikante Anzahl direkter Beschwerden zu Nachrichten erhält, die von Ihrem Konto gesendet wurden, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie das Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt. Wenn wir Ihnen zustimmen, dass die von Ihnen vorgenommenen Änderungen für das Problem angemessen sind, beenden wir den Überprüfungszeitraum für Ihr Konto.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Domain-Blocklist-Benachrichtigungen

In diesem Abschnitt finden Sie zusätzliche Informationen über Domain-Blocklist-Benachrichtigungen, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Die über Ihr Amazon-SES-Konto gesendeten E-Mails enthalten Verweise auf Domänen, die auf einer seriösen Domain Blocklist (DBL) aufgeführt sind. Die Domänen in diesen Listen werden in der Regel mit unerwünschtem oder böswilligem Verhalten in Verbindung gebracht. Bei den fraglichen Domänen handelt es sich möglicherweise um die Domänen, über die Sie E-Mails senden. Nachrichten, die Verweise oder Links zu einer Domäne in einer Domain Blocklist enthalten, werden möglicherweise ebenso markiert wie Nachrichten mit Abbildern, die auf einer solchen Domäne gehostet werden.

Wir können weder die Namen der Domänen bereitstellen, aufgrund derer Ihre Nachricht markiert wird, noch die solchermaßen markierten E-Mails identifizieren.

Wie können Sie das Problem beheben?

Erstellen Sie zunächst eine Liste aller Domänen, auf die in den E-Mails verwiesen wird, die Sie über Amazon SES senden. Bestimmen Sie als Nächstes mit dem Spamhaus Domain Lookup Tool, welche Domänen in Ihrer E-Mail auf der Domain-Blocklist stehen. Möglicherweise werden mehrere der in Ihren E-Mails referenzierten Domänen in der Domain Blocklist aufgeführt.

Die Spamhaus Domain Blocklist ist nicht mit Amazon SES oder verbunden. AWS Wir übernehmen keine Gewähr für die Richtigkeit der Domänen in dieser Liste. Die Spamhaus Domain Blocklist und das Domain Lookup-Tool sind Eigentum von Spamhaus Project und werden von Spamhaus Project betrieben und gepflegt.

Wenn Ihr Konto geprüft wird

In den E-Mails, die Sie während des Überprüfungszeitraums senden, suchen wir nach Verweisen auf Domänen. Wenn Ihre E-Mails immer noch eine beträchtliche Anzahl von Verweisen auf gesperrte Domänen enthalten, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie das Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Gehen Sie in Ihrer Nachricht detailliert auf die von Ihnen vorgenommenen Änderungen ein. Nach Erhalt dieser Nachricht verlängern wir den Überprüfungszeitraum, sodass wir nur die Anzahl der in Ihren E-Mails referenzierten Domänen der Domain-Blocklist analysieren, die nach der Änderungsumsetzung in Ihren E-Mails vorhanden sind. Wenn am Ende dieses erweiterten Überprüfungszeitraums die Anzahl von Domain-Blocklist-Benachrichtigungen deutlich reduziert oder eliminiert wurde und wir glauben, dass Sie Schritte unternommen haben, um zu verhindern, dass dieses Problem zukünftig wieder auftritt, beenden wir den Überprüfungszeitraum für Ihr Konto.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Benachrichtigung zur internen Überprüfung

In diesem Abschnitt finden Sie zusätzliche Informationen über Benachrichtigungen zur internen Überprüfung, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Bei einer umfassenden Überprüfung Ihres Kontos wurden mehrere Punkte ermittelt, die dazu führen könnten, dass E-Mail-Dienstanbieter oder Empfänger Ihre Nachrichten als Spam klassifizieren.

Zum Schutz unserer Prozesse für die Missbrauchserkennung können wir die spezifischen Faktoren, die zu einer solchen Klassifizierung Ihres Kontos geführt haben, nicht offenlegen.

Zu den häufig auftretenden Faktoren für diese Bestimmung zählen folgende:

- Nachrichten, die von kommerziellen Anti-Spam-Systemen markiert werden.
- Nachrichteninhalt, der andeutet, dass der Empfänger diese E-Mail nicht explizit angefordert hat.
- Fehlende Übereinstimmung zwischen dem Absender der Nachricht und dem Branding im E-Mail-Text.
- Inhalt, aus dem der Sender nicht eindeutig hervorgeht.
- Senden von Nachrichten, deren Inhalt auf unerwünschte E-Mails hinweist.
- Formatmuster, die im Zusammenhang mit unerwünschten E-Mails stehen.
- Senden über oder Verweis auf Domänen mit schlechtem Ruf.

Diese Liste ist nicht vollständig. Der spezifische Grund für diese Benachrichtigung kann eine Kombination aus diesen Faktoren sein oder eine andere Ursache haben.

Wie können Sie das Problem beheben?

Die folgenden Vorschläge können den Schweregrad des Problems mindern:

- Stellen Sie sicher, dass Sie E-Mails nur an solche Empfänger senden, die diese E-Mails explizit bei Ihnen angefordert haben.
- Kaufen, mieten oder leihen Sie niemals Listen mit E-Mail-Empfängern.
- Versuchen Sie nicht, Ihre Identität oder den Zweck der Kommunikation in den von Ihnen gesendeten Nachrichten zu verschleiern.
- Erstellen Sie eine Liste mit allen Domänen, auf die Sie in den über Amazon SES gesendeten E-Mails verweisen. Ermitteln Sie mithilfe des Spamhaus Domain Lookup-Tools unter https://www.spamhaus.org/lookup/, ob eine dieser Domänen auf der Spamhaus Domain Blocklist steht.
- Beachten Sie unbedingt die in der Branche bewährten Methoden beim E-Mail-Entwurf.

Diese Liste ist nicht vollständig. Jedoch werden darin einige der wichtigsten Faktoren genannt, die dazu führen können, dass Ihre E-Mails als Spam markiert werden.

Die Spamhaus Domain Blocklist ist nicht mit Amazon SES oder verbunden. AWS Wir übernehmen keine Gewähr für die Richtigkeit der Domänen in dieser Liste. Die Spamhaus Domain Blocklist und

das Domain Lookup-Tool sind Eigentum von Spamhaus Project und werden von Spamhaus Project betrieben und gepflegt.

Wenn Ihr Konto geprüft wird oder wenn die Fähigkeit Ihres Kontos zum Versenden von E-Mails angehalten wurde

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt. Wenn wir Ihnen zustimmen, dass die von Ihnen vorgenommenen Änderungen für das Problem angemessen sind, beenden wir den Überprüfungszeitraum und heben die Sendeunterbrechung für Ihr Konto auf.

Wenn wir nach der Beendigung des Überprüfungszeitraums oder der Sendeunterbrechung für Ihr Konto zu einem späteren Zeitpunkt das gleiche Problem beobachten, legen wir möglicherweise wieder eine Prüfung für Ihr Konto fest oder unterbrechen erneut die Fähigkeit Ihres Kontos zum Versenden von E-Mails. In extremen Fällen oder wenn wir das gleiche Problem mehrfach beobachten, können wir die Fähigkeit Ihres Kontos, E-Mails zu senden, dauerhaft sperren.

Unter Amazon SES Versandprüfungsprozess FAQs finden Sie weitere Informationen zu Verfahren, die Sie anwenden können, wenn Ihr Konto geprüft wird oder die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde.

Benachrichtigung zum E-Mail-Dienstanbieter

In diesem Abschnitt finden Sie zusätzliche Informationen über Benachrichtigungen zum E-Mail-Dienstanbieter, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Ein großer E-Mail-Dienstanbieter hat uns gemeldet, dass unerwünschte oder böswillige E-Mails von einer Adresse oder Domäne, die mit Ihrem Amazon-SES-Konto verknüpft ist, gesendet werden.

Wir können die Identität der Organisation, von der diese Meldung stammt, nicht nennen. Außerdem liegt uns keine Kenntnis über die spezifischen Faktoren vor, auf deren Grundlage der E-Mail-Dienstanbieter die Meldung gemacht hat. In der Regel basiert diese Ermittlung der E-Mail-Dienstanbieter auf Feedback von Kunden, Kundeneinbindungsmetriken, Zustellungsversuchen an ungültige Adressen und von den Spam-Filtern markierter Inhalt. Diese Liste ist nicht vollständig. Möglicherweise hat der E-Mail-Dienstanbieter Ihren Inhalt aufgrund von anderen Faktoren markiert.

Wie können Sie das Problem beheben?

Zur Behebung dieses Problems müssen Sie ermitteln, aufgrund welcher Aspekte Ihres E-Mail-Programms der E-Mail-Dienstanbieter Ihre E-Mail möglicherweise als problematisch einstuft. Anschließend müssen Sie das Programm entsprechend anpassen, um das Problem zu lösen.

Wenn Ihr Konto geprüft wird

Wenn der E-Mail-Anbeiter am Ende des Überprüfungszeitraums die von Ihrem Konto gesendete E-Mail weiterhin als problematisch einstuft, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie das Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Gehen Sie in Ihrer Nachricht detailliert auf die von Ihnen vorgenommenen Änderungen ein. Nach Erhalt dieser Nachricht verlängern wir den Überprüfungszeitraum, sodass wir nur die Benachrichtigungen zu E-Mail-Dienstanbietern analysieren, die nach der Änderungsumsetzung eingegangen sind. Sofern Ihr Konto am Ende des verlängerten Überprüfungszeitraums vom E-Mail-Dienstanbieter nicht mehr als problematisch angesehen wird, können wir möglicherweise den Überprüfungszeitraum für Ihr Konto beenden.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Benachrichtigung zu Empfänger-Feedback

In diesem Abschnitt finden Sie zusätzliche Informationen über Benachrichtigungen zu Empfänger-Feedback, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Ein großer E-Mail-Dienstanbieter hat uns gemeldet, dass sehr viele Benutzer unerwünschte E-Mails von Ihrem Amazon-SES-Konto erhalten und dies dem E-Mail-Dienstanbieter mitgeteilt haben. Diese Art von Feedback wird weder in den direkten Beschwerdeberichten der E-Mail-Dienstanbieter noch in den Unzustellbarkeits- und Beschwerdebenachrichtigungen von Amazon SES erfasst.

Eine hohe Anzahl an Beschwerden kann sich negativ auf alle Amazon-SES-Benutzer auswirken. Um Ihren guten Ruf und den anderer Amazon-SES-Kunden zu schützen, ergreifen wir sofort Maßnahmen, sobald ein Konto eine bestimmte Anzahl an Beschwerden aufweist.

Wir können keine Liste mit den spezifischen E-Mail-Adressen, von denen Ihre E-Mail als unerwünscht gemeldet wurde, vorlegen. Auch den E-Mail-Dienstanbieter, der uns dieses Problem gemeldet hat, können wir nicht namentlich nennen.

Wie können Sie das Problem beheben?

Zur Behebung dieses Problems müssen Sie ermitteln, aufgrund welcher Aspekte Ihres E-Mail-Programms die Empfänger sich möglicherweise über erhaltene E-Mails von Ihnen beschweren. Wenn Sie diese Faktoren identifiziert haben, korrigieren Sie das E-Mail-Sendeverhalten entsprechend.

Es wird empfohlen, bei der Akquise neuer E-Mail-Adressen eine Strategie der doppelten Anmeldung einzusetzen, wie unter Erstellen und Pflegen von Listen beschrieben. Außerdem sollten Sie nur E-Mails an Adressen senden, die diese doppelte Anmeldung ausgeführt haben.

Des Weiteren sollten Sie Adressen aus Ihren Listen löschen, die in letzter Zeit nicht mehr mit Ihren E-Mails interagiert haben. Sie können mithilfe der Nachverfolgungsfunktion für Öffnen und Klicken ermitteln, welche Benutzer die von Ihnen gesendeten Inhalte ansehen und damit interagieren, wie unter Überwachen Ihrer Amazon SES-Sendeaktivität beschrieben.

Wenn Ihr Konto geprüft wird

Wenn der E-Mail-Dienstanbieter am Ende des Überprüfungszeitraums weiterhin eine signifikante Anzahl von Beschwerden meldet, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie das Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Gehen Sie in Ihrer Nachricht detailliert auf die von Ihnen vorgenommenen Änderungen ein. Nach Erhalt dieser Nachricht verlängern wir den

Überprüfungszeitraum, sodass wir nur die Beschwerden der E-Mail-Dienstanbieter analysieren, die nach der Änderungsumsetzung eingegangen sind. Sofern die Anzahl der Beschwerden von E-Mail-Dienstanbietern am Ende des verlängerten Überprüfungszeitraums deutlich reduziert oder eliminiert ist, können wir möglicherweise die Prüfung für Ihr Konto beenden.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Benachrichtigung zu verknüpftem Konto

In diesem Abschnitt finden Sie zusätzliche Informationen über die Benachrichtigungen zu einem verknüpften Konto, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Wir haben ernsthafte Probleme im Zusammenhang mit E-Mails festgestellt, die über ein anderes Amazon-SES-Konto gesendet wurden. Wir glauben, dass das problematische Konto mit Ihrem zusammenhängt. Deshalb haben wir Maßnahmen ergriffen AWS-Konto, um ähnliche Probleme zu vermeiden.

Wie können Sie das Problem beheben?

Wenn wir die Fähigkeit eines Kontos zum Versenden von E-Mails unterbrechen, senden wir immer Informationen über die Gründe für die Sendeunterbrechung an den Eigentümer des betreffenden Kontos. Weitere Informationen finden Sie in der E-Mail, die wir an den Eigentümer des verknüpften Kontos gesendet haben.

Sie sollten zuerst die Probleme mit dem verknüpften Konto angehen. Nachdem Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich

bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt. Wenn wir Ihnen zustimmen, dass die von Ihnen vorgenommenen Änderungen für das Problem angemessen sind, beenden wir den Überprüfungszeitraum und heben die Sendeunterbrechung für Ihr Konto auf.

Benachrichtigung zu Pseudo-E-Mail-Adressen für Spam

In diesem Abschnitt finden Sie zusätzliche Informationen über die Benachrichtigungen zu Pseudo-E-Mail-Adressen für Spam, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Eine externe Anti-Spam-Organisation hat uns gemeldet, dass ihre Pseudo-E-Mail-Adressen für Spam (Spamtraps) kürzlich E-Mails von einer verifizierten Adresse oder von Domänen Ihres Amazon-SES-Kontos erhalten haben.

Bei einer Spamfalle handelt es sich um eine inaktive E-Mail-Adresse, die ausschließlich dazu eingerichtet wurde, Spam-E-Mails zu erhalten. Eine hohe Anzahl an Meldungen zu Pseudo-E-Mail-Adressen für Spam kann sich negativ auf alle Amazon-SES-Benutzer auswirken. Um Ihren guten Ruf und den anderer Amazon-SES-Kunden zu schützen, ergreifen wir sofort Maßnahmen, sobald ein Konto eine bestimmte E-Mail-Anzahl an Pseudo-E-Mail-Adressen für Spam sendet.

Wie können Sie das Problem beheben?

Die E-Mail-Adressen, die mit der gefundenen Spamfalle verknüpft sind, können wir nicht offenlegen. Diese Adressen werden sorgfältig von den Organisationen geschützt, die sie besitzen. Sollten die Adressen bekannt werden, sind sie nutzlos.

Wenn Sie E-Mails an Pseudo-E-Mail-Adressen für Spam senden, ist das meist ein Indikator dafür, dass bei Ihnen ein Problem mit der Beschaffung der kundenseitigen E-Mail-Adressen vorliegt. Beispielsweise können gekaufte E-Mail-Adresslisten Pseudo-E-Mail-Adressen für Spam enthalten; daher ist es gemäß den Amazon-SES-Nutzungsbedingungen nicht zulässig, E-Mails an gekaufte oder gemietete Adresslisten zu senden. Es wird empfohlen, bei der Akquise neuer E-Mail-Adressen eine Strategie der doppelten Anmeldung einzusetzen, wie unter Erstellen und Pflegen von Listen beschrieben. Außerdem sollten Sie nur E-Mails an Adressen senden, die diese doppelte Anmeldung ausgeführt haben.

Des Weiteren sollten Sie Adressen aus Ihren Listen löschen, die in letzter Zeit nicht mehr mit Ihren E-Mails interagiert haben. Sie können mithilfe der Nachverfolgungsfunktion für Öffnen und Klicken ermitteln, welche Benutzer die von Ihnen gesendeten Inhalte ansehen und damit interagieren, wie unter Überwachen Ihrer Amazon SES-Sendeaktivität beschrieben.

Wenn Ihr Konto geprüft wird

Wenn am Ende des Überprüfungszeitraums weiterhin Nachrichten von Ihrem Konto an Spamfallen-Adressen gesendet werden, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie das Problem beheben.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Gehen Sie in Ihrer Nachricht detailliert auf die von Ihnen vorgenommenen Änderungen ein. Nach Erhalt dieser Nachricht verlängern wir den Überprüfungszeitraum, sodass wir nur die Anzahl gemeldeter Pseudo-E-Mail-Adressen für Spam analysieren, die nach der Änderungsumsetzung eingegangen sind. Sofern die Anzahl der Spamfallen-Meldungen am Ende des verlängerten Überprüfungszeitraum deutlich reduziert oder eliminiert wurde, beenden wir möglicherweise die Prüfung für Ihr Konto.

Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde

Sie können anfordern, dass wir diese Entscheidung überdenken. Weitere Informationen finden Sie unter Amazon SES Versandprüfungsprozess FAQs.

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Benachrichtigung zur Websiteanfälligkeit

In diesem Abschnitt finden Sie zusätzliche Informationen über Benachrichtigungen zur Websiteanfälligkeit, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Bei einer umfangreichen Überprüfung wurde festgestellt, dass von Ihrem Konto E-Mail-Nachrichten versendet wurden, die Sie unserer Ansicht nach nicht senden wollten. Diese Nachrichten werden höchstwahrscheinlich von E-Mail-Dienstanbietern und Empfängern als Spam markiert.

In den meisten Fällen wird eine Funktion Ihrer Website von einer Drittpartei zum Senden unerwünschter E-Mails missbraucht. Wenn beispielsweise auf Ihrer Website die Option "E-Mail an einen Freund senden", "Kontakt", "Freunde einladen" oder eine ähnliche Funktion vorhanden ist, kann diese von einem Dritten zum Senden von unerwünschten E-Mails genutzt werden.

Wie können Sie das Problem beheben?

Identifizieren Sie zunächst Funktionen Ihrer Website oder Anwendungen, die von Dritten verwendet werden könnten, um ohne Ihr Wissen E-Mails über Amazon SES zu senden. In Ihrem Supportcenter-Fall können Sie eine Probe der Nachrichten anfordern, von denen wir annehmen, dass sie auf diese Weise gesendet wurden.

Als Nächstes passen Sie die Anwendung oder Website entsprechend an, damit keine unerwünschten E-Mails mehr gesendet werden können. Beispielsweise fügen Sie einen CAPTCHA hinzu, begrenzen die Senderate von E-Mails, entfernen die Option zum Senden von benutzerdefiniertem Inhalt, richten eine obligatorische Benutzeranmeldung zum Senden von E-Mails ein und konfigurieren die Anwendung so, dass nicht mehrere Benachrichtigungen gleichzeitig generiert werden können.

Wenn Ihr Konto geprüft wird oder wenn die Fähigkeit Ihres Kontos zum Versenden von E-Mails angehalten wurde

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Wenn wir nach der Beendigung des Überprüfungszeitraums oder der Sendeunterbrechung für Ihr Konto zu einem späteren Zeitpunkt das gleiche Problem beobachten, legen wir möglicherweise wieder eine Prüfung für Ihr Konto fest oder unterbrechen erneut die Fähigkeit Ihres Kontos

zum Versenden von E-Mails. Wenn wir extreme Probleme oder das gleiche Problem mehrfach beobachten, können wir die Fähigkeit Ihres Kontos, E-Mails zu senden, dauerhaft sperren.

Unter Amazon SES Versandprüfungsprozess FAQs finden Sie weitere Informationen zu Verfahren, die Sie anwenden können, wenn Ihr Konto geprüft wird oder die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde.

Benachrichtigung zu kompromittierten Anmeldeinformationen

In diesem Abschnitt finden Sie zusätzliche Informationen über Benachrichtigungen zu kompromittierten Anmeldeinformationen, die im Amazon-SES-Reputation-Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Bei einer umfangreichen Überprüfung wurde festgestellt, dass von Ihrem Konto E-Mail-Nachrichten versendet wurden, die Sie unserer Ansicht nach nicht senden wollten. Diese Nachrichten werden höchstwahrscheinlich von E-Mail-Dienstanbietern und Empfängern als Spam markiert.

Einige häufige Ursachen sind kompromittierte IAM-Zugriffsschlüssel, kompromittierte SMTP-Passwörter oder andere Sicherheitslücken.

Wie können Sie das Problem beheben?

Sie sollten eine umfassende Sicherheitsüberprüfung Ihrer SES-Nutzungsmechanismen durchführen. Stellen Sie sicher, dass Sie alle entsprechenden SMTP-Passwörter geändert und alle nicht autorisierten Benutzer oder Ressourcen aus Ihrem Konto entfernt haben. Stellen Sie sicher, dass Sie keine sensiblen Informationen wie beispielsweise Passwörter oder Zugriffsschlüssel auf Websites oder Repositorys Dritter speichern. Sie sollten IAM-Zugriffsschlüssel jetzt nicht für Benutzer und niemals für den Root-Benutzer verwenden. Wenn Sie sie noch verwenden, sollten Sie sie auf Mechanismen umstellen, die temporäre Anmeldeinformationen bereitstellen, wie beispielsweise das Erstellen eines Benutzers in AWS IAM Identity Center.

Wenn Ihr Konto geprüft wird oder wenn die Fähigkeit Ihres Kontos zum Versenden von E-Mails angehalten wurde

Wenn Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Nennen Sie darin ausführlich die

Maßnahmen, die Sie zur Problemlösung ergriffen haben, und beschreiben Sie detailliert die Pläne, mit denen sichergestellt werden soll, dass dieses Problem nicht erneut auftritt. Nachdem wir Ihre Anfrage erhalten haben, überprüfen wir die von Ihnen bereitgestellten Informationen und ändern gegebenenfalls den Status Ihres Kontos.

Wenn wir nach der Beendigung des Überprüfungszeitraums oder der Sendeunterbrechung für Ihr Konto zu einem späteren Zeitpunkt das gleiche Problem beobachten, legen wir möglicherweise wieder eine Prüfung für Ihr Konto fest oder unterbrechen erneut die Fähigkeit Ihres Kontos zum Versenden von E-Mails. Wenn wir extreme Probleme oder das gleiche Problem mehrfach beobachten, können wir die Fähigkeit Ihres Kontos, E-Mails zu senden, dauerhaft sperren.

Unter Amazon SES Versandprüfungsprozess FAQs finden Sie weitere Informationen zu Verfahren, die Sie anwenden können, wenn Ihr Konto geprüft wird oder die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen wurde.

Sonstige Benachrichtigung

In diesem Abschnitt finden Sie zusätzliche Informationen über sonstige Benachrichtigungen, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Bei einer automatischen oder von einem Mitarbeiter ausgeführten Überprüfung wurden Probleme festgestellt, die nicht in den vorherigen Abschnitten dieses Dokuments aufgeführt sind.

Wie können Sie das Problem beheben?

Weitere Informationen zu dem spezifischen Problem finden Sie im Supportcenter-Fall, den wir in Ihrem Namen geöffnet haben. Um auf das Support Center zuzugreifen, melden Sie sich beim an AWS-Managementkonsole und wählen Sie dann Support Center. Beschreiben Sie in Ihrer Antwort auf den Fall die Änderungen, die Sie implementiert haben. Abhängig von Ihrer spezifischen Situation und der Art der von uns ermittelten Probleme können wir möglicherweise den Überprüfungszeitraum beenden oder die Fähigkeit Ihres Kontos zum Versenden von E-Mails wiederherstellen.

Erstellen von Alarmen zur Reputationsüberwachung mit CloudWatch

Amazon SES veröffentlicht automatisch eine Reihe von Reputationskennzahlen für Amazon. CloudWatch Sie können anhand dieser Metriken Alarme erstellen, die Sie benachrichtigen, wenn Ihre

Unzustellbarkeits- oder Beschwerdequoten Level erreichen, die Ihre Fähigkeit, E-Mails zu versenden, beeinträchtigen könnten.

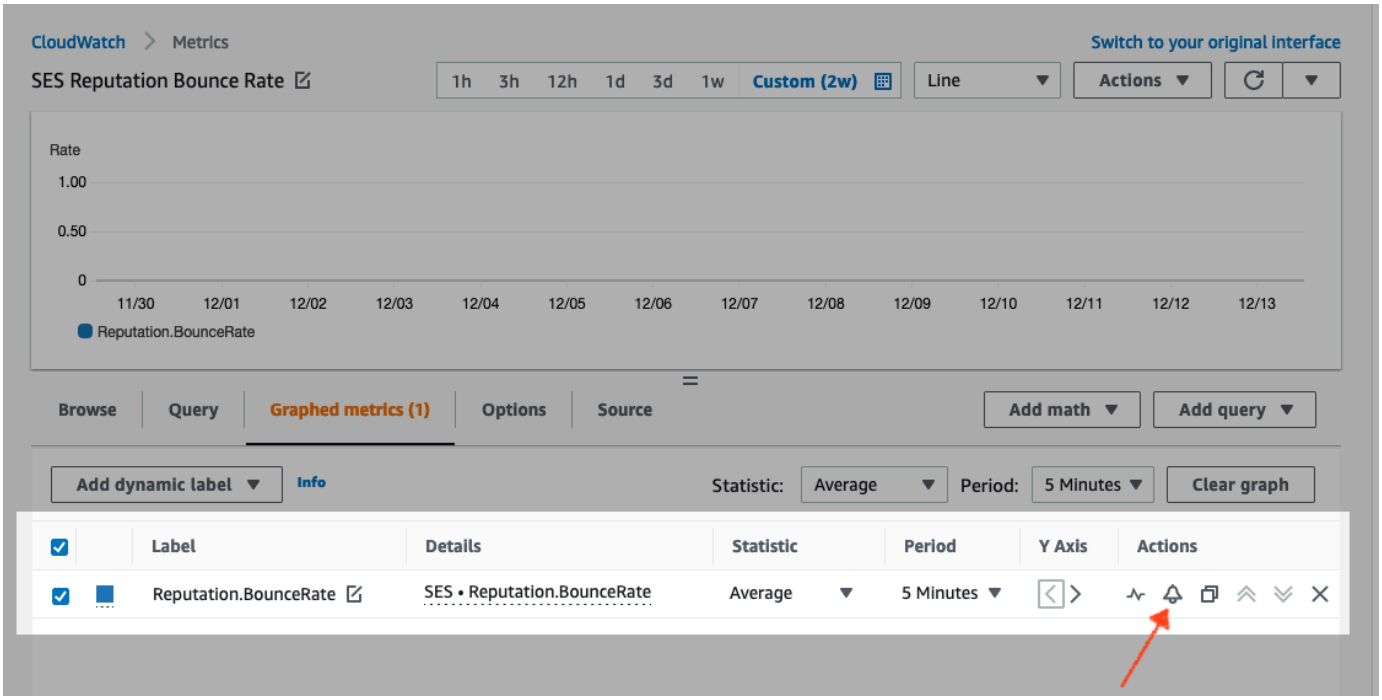
> **Note**
>
> Der CloudWatch Teil der Verfahren in diesem Abschnitt soll lediglich die wichtigsten Schritte zur Einrichtung eines CloudWatch Alarms zur Überwachung Ihrer SES-Absenderreputation erläutern. Sie befassen sich nicht mit erweiterten Konfigurationen in Bezug auf optionale Einstellungen für CloudWatch Alarme. Vollständige Informationen zur Konfiguration von CloudWatch Alarmen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.

Voraussetzungen

- Erstellen Sie ein Amazon-SNS-Thema und abonnieren Sie es dann unter Verwendung des von Ihnen bevorzugten Endpunkts (z. B. E-Mail oder SMS). Weitere Informationen finden Sie unter Erstellen eines Amazon-SNS-Themas und Abonnieren eines Amazon-SNS-Themas im Entwicklerhandbuch für Amazon Simple Notification Service.
- Wenn Sie in der aktuellen Region noch nie eine E-Mail gesendet haben, wird der SES-Namespace möglicherweise nicht angezeigt. Um sicherzustellen, dass Sie über Metriken verfügen, senden Sie eine Test-E-Mail an den Postfachsimulator.

Um einen CloudWatch Alarm zur Überwachung der Versandreputation zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich auf der linken Seite des Bildschirms die Option Reputation Dashboard aus.
3. Wählen Sie auf der Seite mit den Reputationskennzahlen auf der Registerkarte Kontoebene entweder im Bereich Absprungrate oder Beschwerderate die Option Anzeigen in CloudWatch aus. Dadurch wird die CloudWatch Konsole mit der von Ihnen ausgewählten Kennzahl geöffnet.
4. Klicken Sie auf der Registerkarte Graphische Messwerte auf die Zeile mit der von Ihnen ausgewählten Kennzahl, in diesem Beispiel Reputation. BounceRate, wählen Sie das Alarmglockensymbol in der Spalte „Aktionen“ (siehe Abbildung unten). Dadurch wird die Seite „Metrik und Bedingungen angeben“ geöffnet.



5. Blättern Sie nach unten bis zum Abschnitt Bedingungen und wählen Sie Statisch im Feld Typ des Schwellenwerts.

   a. Im Fenster Whenever ***`metric`*** is... Wählen Sie im Feld Größer/Gleich aus.

   b. Im als... Feld, geben Sie den Wert CloudWatch an, der einen Alarm auslösen soll.

      - Wenn Sie einen Alarm zur Überwachung Ihrer Unzustellbarkeitsquote erstellen, ist zu beachten, dass Amazon SES Ihnen empfiehlt, die Unzustellbarkeitsquote unter 5 % zu halten. Wenn die Unzustellbarkeitsquote für Ihr Konto größer als 10 % ist, kann es sein, dass wir die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrechen. Aus diesem Grund sollten Sie so konfigurieren, CloudWatch dass Sie eine Benachrichtigung erhalten, wenn die Absprungrate für Ihr Konto größer oder gleich 0,05 (5%) ist.
      - Wenn Sie einen Alarm zur Überwachung Ihrer Beschwerdequote erstellen, ist zu beachten, dass Amazon SES Ihnen empfiehlt, die Beschwerdequote unter 0,1 % zu halten. Wenn die Beschwerdequote für Ihr Konto größer als 0,5 % ist, kann es sein, dass wir die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrechen. Aus diesem Grund sollten Sie so konfigurieren, CloudWatch dass Sie eine Benachrichtigung erhalten, wenn die Beschwerderate für Ihr Konto größer oder gleich 0,001 (0,1%) ist.

   c. Erweitern Sie zusätzliche Konfiguration und wählen Sie im Feld Behandlung fehlender Daten die Option Fehlende Daten als ignorieren behandeln (Alarmzustand beibehalten).

   d. Wählen Sie Weiter aus.

6. Wählen Sie im Bereich Aktionen konfigurieren in Alarm im Feld Alarmzustandsauslöser.
   a. Wählen Sie Select an SNS topic (SNS-Thema auswählen) im Feld Select an existing SNS topic (Vorhandenes SNS-Thema auswählen).
   b. Wählen Sie das Thema, das Sie erstellt und in den Voraussetzungen im Suchfeld Benachrichtigung senden an... abonniert haben.
   c. Wählen Sie Weiter aus.
7. Geben Sie im Abschnitt Name und Beschreibung hinzufügen einen Namen und eine Beschreibung für den Alarm ein und wählen Sie Next (Weiter).
8. Bestätigen Sie im Abschnitt Vorschau und erstellen Ihre Einstellungen und wenn Sie zufrieden sind, wählen Sie Alarm erstellen aus. Wenn es etwas gibt, das Sie ändern möchten, wählen Sie die Vorherige-Schaltfläche für jeden Abschnitt, zu dem Sie zurückkehren und ihn bearbeiten möchten.

SNDS-Metriken für dedizierte IPs

Sie können Smart Network Data Services (SNDS) -Daten für geleaste dedizierte IP-Adressen in allen Bereichen anzeigen, in AWS-Region denen Sie Amazon SES verwenden. Diese SNDS-Daten sind über die CloudWatch Amazon-Konsole verfügbar.

SNDS ist ein Outlook-Programm, mit dem IP-Besitzer Spam in ihrem IP-Bereich verhindern können. Amazon SES stellt diese wichtigen Daten für diejenigen bereit, die Dedicated leasen IPs. Die SNDS-Daten bieten Einblicke in das E-Mail-Versandverhalten der IP und weisen auf Bereiche hin, die Ihre Absenderzuverlässigkeit beeinträchtigen können.

> **Note**
>
> In Bezug auf Outlook deckt dies alle Domänen ab, die sie verfolgen. Dies kann beispielsweise Hotmail.com, Outlook.com und Live.com umfassen.

SNDS-Daten für Ihre dedizierten IP-Adressen anzeigen

1. Melden Sie sich bei der CloudWatch Amazon-Konsole unter an https://console.aws.amazon.com/cloudwatch/.
2. Erweitern Sie im Navigationsbereich Metrics (Metriken) und wählen Sie dann All metrics (Alle Metriken) aus.

(Es werden Anweisungen für die neue CloudWatch Konsolenoberfläche gegeben.)

3. Wählen Sie auf der Registerkarte Durchsuchen im Metrikcontainer Ihre aus AWS-Region und wählen Sie dann SES aus.
4. Wählen Sie IP-Metriken aus, um Ihnen all Ihre von SNDS IPs verfolgten Daten anzuzeigen.

   (Hinweis: Wenn Ihrem Konto in der ausgewählten Region keine dedizierten IP-Adressen zugeordnet sind, werden IP-Metriken nicht in der CloudWatch Konsole angezeigt.)
5. Sehen Sie sich in dieser Liste all Ihre von SNDS IPs verfolgten dedizierten IP-Adressen an oder wählen Sie eine einzelne IP-Adresse aus, um nur deren Metriken zu sehen.

Die folgenden Metriken werden für jede dedizierte IP-Adresse bereitgestellt und von Outlook definiert. Weitere Informationen finden Sie unter FAQsSNDS von Outlook.

> **Note**
>
> Diese Metriken stellen einen Aktivitätszeitraum dar, der einmal täglich aktualisierte Daten bereitstellt. Die Metriken haben auch einen entsprechenden Zeitstempel, der einen Zeitraum von 24 Stunden widerspiegelt.

- SNDS. RCPTCommands - Dies ist die Anzahl der RCPT-Befehle, die SNDS für die spezifische IP-Adresse während des Aktivitätszeitraums erkannt hat. RCPT-Befehle sind Teil des SMTP-Protokolls, das zum Senden von E-Mails verwendet wird und das die Empfängeradresse angibt, an die Sie E-Mails senden möchten.
- SNDS. DATACommands - Die Anzahl der DATA-Befehle, die SNDS für die spezifische IP-Adresse während des Aktivitätszeitraums erkannt hat. DATA-Befehle sind Teil des SMTP-Protokolls, das zum Senden von E-Mails verwendet wird, insbesondere jener Teil, der die Nachricht tatsächlich an die zuvor festgelegten Empfänger überträgt.
- SNDS. MessageRecipients - Die Anzahl der Empfänger von Nachrichten, die SNDS für die spezifische IP-Adresse während des Aktivitätszeitraums wahrgenommen hat.
- SNDS. SpamRate - Zeigt die Gesamtergebnisse der Spam-Filterung an, die auf alle Nachrichten angewendet wurde, die von der IP-Adresse während des angegebenen Aktivitätszeitraums gesendet wurden.
  - Ein SpamRate Wert von 0 bedeutet, dass die IP-Adresse weniger als 10% Spam enthält.

  - Ein SpamRate Wert von 0,5 bedeutet, dass zwischen 10 und 90% Spam von der IP-Adresse generiert wird.
  - Ein SpamRate Wert von 1 bedeutet, dass 90% oder mehr Spam von der IP-Adresse generiert werden.
- SENDET. ComplaintRate - Dies ist der Bruchteil der Zeit, in der sich ein Outlook-Benutzer während des Aktivitätszeitraums über eine von der IP empfangene Nachricht beschwert.
  - Ein ComplaintRate Wert von 1 bedeutet eine Beschwerdequote von 100%.
  - Ein ComplaintRate Wert von 0,05 würde beispielsweise eine Beschwerdequote von 5% bedeuten.
  - Ein Wert ComplaintRate von 0 bedeutet, dass die Quote unter 0,1% liegt.
- SENDET. TrapHits - Zeigt die Anzahl der Nachrichten an, die an „Trap-Konten“ gesendet wurden. Trap-Konten sind Konten, die von Outlook verwaltet werden, die keine E-Mails anfordern. Daher sind alle Nachrichten, die an Trap-Konten gesendet werden, sehr wahrscheinlich Spam.

Vorschläge für die Fehlerbehebung

F1. Warum werden Daten nicht jeden Tag aufgefüllt? Eines der folgenden Szenarien könnte zutreffen:

- SNDS-Daten sind vom Outlook-SNDS-Programm abhängig.
- Es gibt einen Mindestschwellenwert für E-Mails, die SNDS empfangen muss, um einen Wert zu berechnen. Daten sind möglicherweise nicht in Zeiten verfügbar, in denen das E-Mail-Volumen auf einer IP gering war.

F2. Warum sind die SNDS. SpamRate und SNDS. ComplaintRate Metriken ändern sich, und was mache ich, wenn sich die Rate auf einen Wert von 1 ändert?

Dies ist ein Indikator, dass etwas in Ihrem Sendeverhalten eine negative Antwort aus dem Outlook-SNDS-Programm ausgelöst hat. In diesem Fall sollten Sie auch andere Internetdienstanbieter (ISPs) sowie Ihre Nutzerzahlen überprüfen, um sicherzustellen, dass es sich nicht um ein globales Problem handelt. Wenn es sich um ein globales Problem handelt, treten möglicherweise Probleme mit mehreren auf ISPs, was auf ein Listen-, Inhalts-, Verteilungs- oder Berechtigungsproblem hindeuten würde. Wenn es sich speziell um Outlook handelt, lesen Sie die empfohlenen Richtlinien für Outlook.

F3. Welche Maßnahmen werden AWS Support ergriffen, wenn mein SNDS. SpamRate wechselt von einem Wert von 0 (oder 0,5) auf 1?

AWS hat keine Kontrolle über SNDS und hat daher keinen Einfluss auf SNDS. Alle Anforderungen zu Abhilfemaßnahmen müssen direkt bei Outlook über das Formular für eine neue Support-Anfrage eingereicht werden.

Automatisches Unterbrechen des E-Mail-Versands

Um Ihren Ruf als Absender zu schützen, können Sie den E-Mail-Versand für Nachrichten, die mit bestimmten Konfigurationssätzen gesendet wurden, oder für alle Nachrichten, die von Ihrem Amazon SES SES-Konto in einer bestimmten AWS Region gesendet wurden, vorübergehend unterbrechen.

Mithilfe von Amazon CloudWatch und Lambda können Sie eine Lösung erstellen, die den E-Mail-Versand automatisch pausiert, wenn Ihre Reputationsmetriken (wie Absprungrate oder Beschwerderate) bestimmte Schwellenwerte überschreiten. In diesem Thema werden die Verfahren zum Einrichten dieser Lösung beschrieben.

Themen in diesem Abschnitt:

- Automatisches Pausieren des E-Mail-Versands für Ihr gesamtes Amazon-SES-Konto
- Automatisches Pausieren des E-Mail-Versands für einen Konfigurationssatz

Automatisches Pausieren des E-Mail-Versands für Ihr gesamtes Amazon-SES-Konto

In den Verfahren in diesem Abschnitt werden die Schritte zur Einrichtung von Amazon SES, Amazon SNS CloudWatch, Amazon und AWS Lambda zur automatischen Unterbrechung des E-Mail-Versands für Ihr Amazon SES SES-Konto in einer einzelnen AWS Region erläutert. Wenn Sie E-Mails aus mehreren Regionen versenden, wiederholen Sie die Verfahren in diesem Abschnitt für jede Region, in der Sie diese Lösung implementieren möchten.

Themen in diesem Abschnitt:

- Teil 1: Erstellen einer IAM-Rolle
- Teil 2: Erstellen der Lambda-Funktion
- Teil 3: Erneutes Aktivieren des E-Mail-Versands für Ihr Konto
- Teil 4: Erstellen eines Amazon-SNS-Themas und -Abonnements
- Teil 5: Einen Alarm erstellen CloudWatch
- Teil 6: Testen der Lösung

Teil 1: Erstellen einer IAM-Rolle

Der erste Schritt für die Konfiguration der automatischen Pausierung des E-Mail-Versands besteht darin, eine IAM-Rolle zu erstellen, welche die `UpdateAccountSendingEnabled`-API-Operation ausführen kann.

So erstellen Sie die IAM-Rolle

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie auf der Seite Select trusted entity (Auswahl der vertrauenswürdigen Entität) unter Trusted entity type (Auswahl der vertrauenswürdigen Entität) die Option AWS service (AWS - Service) aus.
5. Wählen Sie unter Use case (Anwendungsfall) die Option Lambda und dann Next (Weiter) aus.
6. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die folgenden Richtlinien aus:

   - AWSLambdaBasicExecutionRole
   - SESFullZugriff auf Amazon

   > **Tip**
   >
   > Verwenden Sie das Suchfeld unter Permission policies (Berechtigungsrichtlinien), um diese Richtlinien schnell zu finden. Beachten Sie jedoch, dass Sie nach der Suche und Auswahl der ersten Richtlinie die Option Clear (Löschen) auswählen müssen, bevor Sie die zweite Richtlinie suchen und auswählen.

   Klicken Sie anschließend auf Weiter.
7. Geben Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) unter Role details (Rollendetails) einen aussagekräftigen Namen für die Richtlinie im Feld Role name (Rollenname) ein.
8. Stellen Sie sicher, dass die beiden Richtlinien in der Tabelle Permissions policy summary (Berechtigungsrichtlinienübersicht) ausgewählt sind, und wählen Sie dann Create role (Rolle erstellen) aus.

Teil 2: Erstellen der Lambda-Funktion

Nachdem Sie eine IAM-Rolle erstellt haben, können Sie die Lambda-Funktion erstellen, mit der das Senden von E-Mails für Ihr Konto pausiert wird.

So erstellen Sie die Lambda-Funktion:

1. Öffnen Sie die AWS Lambda Konsole unter https://console.aws.amazon.com/lambda/.
2. Wählen Sie mithilfe der Regionsauswahl die Region aus, in der Sie diese Lambda-Funktion bereitstellen möchten.

   > **Note**
   >
   > Diese Funktion unterbricht nur den E-Mail-Versand in der AWS Region, die Sie in diesem Schritt ausgewählt haben. Wenn Sie aus mehr als einer Region E-Mails versenden, wiederholen Sie die Verfahren in diesem Abschnitt für jede Region, in der das Senden von E-Mails automatisch pausiert werden soll.

3. Wählen Sie Create function (Funktion erstellen).
4. Wählen Sie unter Create function (Funktion erstellen) die Option Author from scratch (Scratch-Autor).
5. Führen Sie auf der Seite Basic information (Grundlegende Informationen) folgende Schritte aus:

   - Geben Sie für Function name (Funktionsname) einen Namen für die Lambda-Funktion ein.
   - Bei Laufzeit wählen Sie Node.js 18x(oder die Version, die derzeit in der Auswahlliste angeboten wird) aus.
   - Behalten Sie für Architecture (Architektur) den vorab ausgewählten Standardnamen x86_64bei.
   - Erweitern Sie die Option Change default execution role (Standardausführungsrolle ändern) unter „Permissions“ (Berechtigungen) und wählen Sie Use an existing role (Vorhandene Rolle verwenden) aus.
   - Klicken Sie in das Feld Existing role (Vorhandene Rolle) und wählen Sie die IAM-Rolle aus, die Sie in the section called “Teil 1: Erstellen einer IAM-Rolle” erstellt haben.

   Wählen dann Sie Funktion erstellen.
6. Fügen Sie im Code-Editor unter Code source (Codequelle) den folgenden Code ein:

```
'use strict';


const { SES } = require("@aws-sdk/client-ses")

// Create a new SES object.

var ses = new SES({});

// Specify the parameters for this operation. In this case, there is only one
// parameter to pass: the Enabled parameter, with a value of false
// (Enabled = false disables email sending, Enabled = true enables it).
var params = {
    Enabled: false
};

exports.handler = (event, context, callback) => {
    // Pause sending for your entire SES account
    ses.updateAccountSendingEnabled(params, function(err, data) {
        if(err) {
            console.log(err.message);
        } else {
            console.log(data);
        }
    });
};
```

Wählen Sie dann Deploy (Bereitstellen) aus.

7. Wählen Sie Test aus. Wenn das Fenster Configure test event (Testereignis konfigurieren) angezeigt wird, geben Sie einen Namen im Feld Event name (Ereignisname) ein und wählen Sie dann Save (Speichern) aus.
8. Erweitern Sie das Dropdown-Feld Test (Testen) und wählen Sie den Ereignisnamen aus, den Sie gerade erstellt haben. Wählen Sie dann Test (Testen) aus.
9. Die Registerkarte Execution results (Ausführungsergebnisse) erscheint. Vergewissern Sie sich, dass direkt darunter und rechts `Status: Succeeded` angezeigt wird. Wenn die Funktion nicht ausgeführt werden kann, führen Sie die folgenden Schritte aus:

   - Überprüfen Sie, ob die IAM-Rolle, die Sie in the section called “Teil 1: Erstellen einer IAM-Rolle” erstellt haben, die richtigen Richtlinien enthält.

- Vergewissern Sie sich, dass der Code in der Lambda-Funktion keine Syntaxfehler enthält. Der Lambda-Code-Editor hebt automatisch Syntaxfehler und andere potenzielle Probleme hervor.

Teil 3: Erneutes Aktivieren des E-Mail-Versands für Ihr Konto

Ein Nebeneffekt des Testens der Lambda-Funktion in the section called “Teil 2: Erstellen der Lambda-Funktion” besteht darin, dass das Versenden von E-Mails für Ihr Amazon-SES-Konto angehalten wird. In den meisten Fällen möchten Sie den Versand für Ihr Konto nicht unterbrechen, bis der CloudWatch Alarm ausgelöst wird.

Mithilfe der Verfahren in diesem Abschnitt wird der E-Mail-Versand für Ihr Amazon-SES-Konto erneut aktiviert. Um diese Verfahren ausführen zu können, müssen Sie die AWS Command Line Interface installieren und konfigurieren. Weitere Informationen finden Sie im AWS Command Line Interface - Benutzerhandbuch.

So aktivieren Sie das Senden von E-Mails erneut

1. Geben Sie in der Befehlszeile den folgenden Befehl ein, um das Senden von E-Mails für Ihr Konto erneut zu aktivieren: *sending_region*Ersetzen Sie es durch den Namen der Region, in der Sie den E-Mail-Versand wieder aktivieren möchten.

   ```
   aws ses update-account-sending-enabled --enabled --region sending_region
   ```

2. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den Status des E-Mail-Versands für Ihr Konto zu überprüfen:

   ```
   aws ses get-account-sending-enabled --region sending_region
   ```

   Wenn die folgende Meldung ausgegeben wird, haben Sie das Senden von E-Mails für Ihr Konto erfolgreich erneut aktiviert:

   ```
   {
       "Enabled": true
   }
   ```

Teil 4: Erstellen eines Amazon-SNS-Themas und -Abonnements

CloudWatch Damit Sie Ihre Lambda-Funktion ausführen können, wenn ein Alarm ausgelöst wird, müssen Sie zunächst ein Amazon SNS SNS-Thema erstellen und die Lambda-Funktion abonnieren.

So erstellen Sie das Amazon-SNS-Thema und abonnieren die Lambda-Funktion dazu

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Erstellen Sie ein Thema, indem Sie den Schritten im Entwicklerhandbuch für Amazon Simple Notification Service folgen.
   - Der Type (Typ) muss Standard sein (nicht FIFO).
3. Erstellen Sie ein Thema, indem Sie den Schritten im Entwicklerhandbuch für Amazon Simple Notification Service folgen.
   a. Wählen Sie unter Protocol (Protokoll) die Option AWS Lambda aus.
   b. Wählen Sie für Endpoint (Endpunkt) die Lambda-Funktion aus, die Sie in the section called “Teil 2: Erstellen der Lambda-Funktion” erstellt haben.

Teil 5: Einen Alarm erstellen CloudWatch

Dieser Abschnitt enthält Verfahren zum Erstellen eines Alarms CloudWatch , der ausgelöst wird, wenn eine Metrik einen bestimmten Schwellenwert erreicht. Wenn der Alarm ausgelöst wird, übermittelt er eine Benachrichtigung an das the section called “Teil 4: Erstellen eines Amazon-SNS-Themas und -Abonnements”-Thema, das Sie in Amazon SNS erstellt haben, was dann wiederum die Lambda-Funktion auslöst, die Sie in the section called “Teil 2: Erstellen der Lambda-Funktion” erstellt haben.

Um einen CloudWatch Alarm zu erstellen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie mithilfe der Regionsauswahl die Region aus, in der Sie den E-Mail-Versand automatisch pausieren möchten.
3. Klicken Sie im Navigationsbereich auf Alarms (Alarme).
4. Wählen Sie Create Alarm (Alarm erstellen) aus.
5. Wählen Sie im Fenster Create Alarm (Alarm erstellen) unter SES Metrics (SES-Metriken) die Option Account Metrics (Kontenmetriken) aus.

6. Wählen Sie unter Metric Name (Metrikname) eine der folgenden Optionen aus:

   - Ruf. BounceRate — Wählen Sie diese Metrik, wenn Sie den E-Mail-Versand für Ihr Konto unterbrechen möchten, wenn die allgemeine Hard-Bounce-Rate für Ihr Konto einen von Ihnen definierten Schwellenwert überschreitet.
   - Ruf. ComplaintRate — Wählen Sie diese Metrik, wenn Sie den E-Mail-Versand für Ihr Konto unterbrechen möchten, wenn die allgemeine Beschwerderate für Ihr Konto einen von Ihnen definierten Schwellenwert überschreitet.

   Wählen Sie Weiter aus.

7. Führen Sie folgende Schritte aus:

   - Geben Sie unter Alarm Threshold (Alarm-Schwellenwert) im Feld Name einen Namen für den Alarm ein.
   - Unter Wann auch immer: Ruf. BounceRateOder wann auch immer: Ruf. ComplaintRate, geben Sie den Schwellenwert an, durch den der Alarm ausgelöst wird.

     > **Note**
     >
     > Ihr Konto wird automatisch überprüft, wenn Ihre Absprungrate 5% oder Ihre Beschwerderate 0,1% übersteigt. Wenn Sie die Absprungs- oder Beschwerdequote angeben, aufgrund derer der CloudWatch Alarm ausgelöst wird, empfehlen wir Ihnen, Werte zu verwenden, die unter diesen Raten liegen, um zu verhindern, dass Ihr Konto überprüft wird.

   - Wählen Sie unter Actions (Aktionen) für Whenever this alarm die Option State is ALARM (Status ist ALARM) aus. Wählen Sie für Send notification to (Benachrichtigung senden an) das Amazon-SNS-Thema aus, das Sie in the section called “Teil 4: Erstellen eines Amazon-SNS-Themas und -Abonnements” erstellt haben.

   Wählen Sie Alarm erstellen aus.

Teil 6: Testen der Lösung

Sie können jetzt den Alarm testen, um sicherzustellen, dass er die Lambda-Funktion ausführt, wenn er in den Status `ALARM` versetzt wird. Sie können die API-Operation `SetAlarmState` verwenden, um den Status des Alarms temporär zu ändern.

Die Verfahren in diesem Abschnitt sind optional, es wird jedoch empfohlen, diese durchzuführen, um sicherzustellen, dass die gesamte Lösung ordnungsgemäß konfiguriert ist.

1. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den Status des E-Mail-Versands für Ihr Konto zu überprüfen: *region*Ersetzen Sie es durch den Namen der Region.

   ```
   aws ses get-account-sending-enabled --region region
   ```

   Wenn der Versand für Ihr Konto aktiviert ist, wird die folgende Meldung ausgegeben:

   ```
   {
       "Enabled": true
   }
   ```

2. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den Alarmstatus vorübergehend in `ALARM` zu ändern: aws cloudwatch set-alarm-state --alarm-name ***MyAlarm*** --state-value ALARM --state-reason "Testing execution of Lambda function" --region ***region***

   Ersetzen *MyAlarm* Sie den vorherigen Befehl durch den Namen des Alarmsthe section called “Teil 5: Einen Alarm erstellen CloudWatch”, in dem Sie ihn erstellt haben, und *region* durch die Region, in der Sie den E-Mail-Versand automatisch unterbrechen möchten.

   > **Note**
   >
   > Wenn Sie diesen Befehl ausführen, wechselt der Status des Alarms innerhalb weniger Sekunden von `OK` zu `ALARM` und zurück zu `OK`. Sie können diese Statusänderungen auf der Registerkarte Verlauf des Alarms in der CloudWatch Konsole oder mithilfe der DescribeAlarmHistoryOperation anzeigen.

3. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den Status des E-Mail-Versands für Ihr Konto zu überprüfen:

   ```
   aws ses get-account-sending-enabled --region region
   ```

Wenn die Lambda-Funktion erfolgreich ausgeführt wird, wird die folgende Meldung ausgegeben:

```
{
    "Enabled": false
}
```

4. Führen Sie die Schritte in the section called “Teil 3: Erneutes Aktivieren des E-Mail-Versands für Ihr Konto” aus, um den E-Mail-Versand für Ihr Konto erneut zu aktivieren.

Automatisches Pausieren des E-Mail-Versands für einen Konfigurationssatz

Sie können Amazon SES so konfigurieren, dass Reputationsmetriken exportiert werden, die spezifisch für E-Mails sind, die mit einer bestimmten Konfiguration an Amazon gesendet werden CloudWatch. Sie können diese Metriken dann verwenden, um CloudWatch Alarme zu erstellen, die für diese Konfigurationssätze spezifisch sind. Wenn diese Alarme bestimmte Grenzwerte überschreiten, können Sie das Senden von den E-Mails automatisch pausieren, welche die angegebenen Konfigurationssätze verwenden, ohne die gesamten Fähigkeiten zum E-Mail-Versand Ihres Amazon-SES-Kontos zu beeinträchtigen.

> **Note**
>
> Die in diesem Abschnitt beschriebene Lösung unterbricht den E-Mail-Versand für einen bestimmten Konfigurationssatz in einer einzelnen AWS Region. Wenn Sie E-Mails aus mehreren Regionen versenden, wiederholen Sie die Verfahren in diesem Abschnitt für jede Region, in der Sie diese Lösung implementieren möchten.

Themen in diesem Abschnitt:

- Teil 1: Aktivieren Sie die Berichterstattung der Zuverlässigkeitsmetriken für den Konfigurationssatz
- Teil 2: Erstellen einer IAM-Rolle
- Teil 3: Erstellen der Lambda-Funktion
- Teil 4: Erneute Aktivierung des E-Mail-Versands für den Konfigurationssatz
- Teil 5: Erstellen eines Amazon-SNS-Themas
- Teil 6: Einen Alarm erstellen CloudWatch
- Teil 7: Testen der Lösung

Teil 1: Aktivieren Sie die Berichterstattung der Zuverlässigkeitsmetriken für den Konfigurationssatz

Bevor Sie Amazon SES konfigurieren, um das Senden von E-Mails für einen Konfigurationssatz automatisch zu pausieren, müssen Sie zuerst den Export der Zuverlässigkeitsmetriken für den Konfigurationssatz aktivieren.

Führen Sie für die Aktivierung des Exports von Unzustellbarkeits -und Beschwerdemetriken für den Konfigurationssatz die Schritte in the section called “Reputationsmetriken anzeigen und exportieren” aus.

Teil 2: Erstellen einer IAM-Rolle

Der erste Schritt für die Konfiguration der automatischen Pausierung des E-Mail-Versands besteht darin, eine IAM-Rolle zu erstellen, welche die `UpdateConfigurationSetSendingEnabled`-API-Operation ausführen kann.

So erstellen Sie die IAM-Rolle

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität auswählen) die Option AWS -Service aus.
5. Wählen Sie unter Choose the service that will use this role (Die Rolle auswählen, die diese Rollen verwenden wird) die Option Lambda aus. Wählen Sie Next: Permissions (Weiter: Berechtigungen) aus.
6. Wählen Sie auf der Seite Attach permissions policies (Berechtigungsrichtlinien anfügen) die folgenden Richtlinien aus:

   - AWS Lambda BasicExecutionRole
   - Amazon SESFull Access (Wir empfehlen Ihnen, eine benutzerdefinierte Rolle zu verwenden, die auf Ihre Bedürfnisse zugeschnitten ist und Anrufberechtigungen beinhaltet `UpdateConfigurationSetSendingEnabled`.)

> **Tip**
>
> Verwenden Sie das Suchfeld oben in der Liste der Richtlinien, um diese Richtlinien schnell zu finden.

Klicken Sie auf Next: Review (Weiter: Überprüfen).

7. Geben Sie auf der Seite Review (Überprüfen) im Feld Name einen Namen für die Rolle ein. Wählen Sie Create role (Rolle erstellen) aus.

Teil 3: Erstellen der Lambda-Funktion

Nachdem Sie eine IAM-Rolle erstellt haben, können Sie die Lambda-Funktion erstellen, mit der das Senden von E-Mails für den Konfigurationssatz pausiert wird.

So erstellen Sie die Lambda-Funktion:

1. Öffnen Sie die AWS Lambda Konsole unter https://console.aws.amazon.com/lambda/.
2. Wählen Sie mithilfe der Regionsauswahl die Region aus, in der Sie diese Lambda-Funktion bereitstellen möchten.

> **Note**
>
> Diese Funktion pausiert nur das Senden von E-Mails für Konfigurationssätze in der AWS -Region, die Sie in diesem Schritt auswählen. Wenn Sie aus mehr als einer Region E-Mails versenden, wiederholen Sie die Verfahren in diesem Abschnitt für jede Region, in der das Senden von E-Mails automatisch pausiert werden soll.

3. Wählen Sie Create function (Funktion erstellen).
4. Wählen Sie unter Create function (Funktion erstellen) die Option Author from scratch (Scratch-Autor).
5. Führen Sie unter Author from scratch (Scratch-Autor) die folgenden Schritte durch:

   - Geben Sie für Name einen Namen für die Lambda-Funktion ein.

- Bei Laufzeit wählen Sie Node.js 14x(oder die Version, die derzeit in der Auswahlliste angeboten wird) aus.
- Wählen Sie für Role (Rolle) die Option Choose an existing role (Vorhandene Rolle auswählen).
- Wählen Sie für Existing role (Vorhandene Rolle) die IAM-Rolle aus, die Sie in the section called “Teil 2: Erstellen einer IAM-Rolle” erstellt haben.

Wählen Sie Funktion erstellen.

6. Fügen Sie sie im Code-Editor unter Function code (Funktionscode) den folgenden Code ein:

```
'use strict';

import {
    SES
}
from 'aws-sdk';

const ses = new SES();
const configSet = 'CONFIG_SET_NAME_HERE';

const params = {
    ConfigurationSetName: configSet,
    Enabled: false
};

export const handler = async (event) => {
    try {
        const data = await
 ses.updateConfigurationSetSendingEnabled(params).promise();

        console.log('Configuration Set Update:', data);

        return {
            statusCode: 200,
            body: JSON.stringify({
                message: 'Successfully paused email sending for configuration
 set.',
                data
            }),
        };
    }
    catch (err) {
```

```
        console.error('Error:', err.message);
        return {
            statusCode: 500,
            body: JSON.stringify({
                message: 'Failed to pause email sending for configuration set.',
                error: err.message
            }),
        };
    }
};
```

Ersetzen Sie *ConfigSet* den obigen Code durch den Namen des Konfigurationssatzes. Wählen Sie Speichern.

7. Wählen Sie Test aus. Wenn das Fenster Configure test event (Testereignis konfigurieren) angezeigt wird, geben Sie einen Namen im Feld Event name (Ereignisname) ein und wählen Sie dann Create (Erstellen) aus.
8. Stellen Sie sicher, dass die Benachrichtigungsleiste oben auf der Seite `Execution result: succeeded` anzeigt. Wenn die Funktion nicht ausgeführt werden kann, führen Sie die folgenden Schritte aus:

   - Überprüfen Sie, ob die IAM-Rolle, die Sie in the section called “Teil 2: Erstellen einer IAM-Rolle” erstellt haben die richtigen Richtlinien enthält.
   - Vergewissern Sie sich, dass der Code in der Lambda-Funktion keine Syntaxfehler enthält. Der Lambda-Code-Editor hebt automatisch Syntaxfehler und andere potenzielle Probleme hervor.

Teil 4: Erneute Aktivierung des E-Mail-Versands für den Konfigurationssatz

Ein Nebeneffekt des Tests der Lambda-Funktion in the section called “Teil 3: Erstellen der Lambda-Funktion” ist, dass das Senden von E-Mails für den Konfigurationssatz pausiert ist. In den meisten Fällen möchten Sie das Senden für den Konfigurationssatz nicht unterbrechen, bis der CloudWatch Alarm ausgelöst wird.

Mithilfe der Verfahren in diesem Abschnitt wird der E-Mail-Versand für Ihren Konfigurationssatz erneut aktiviert. Um diese Verfahren ausführen zu können, müssen Sie die AWS Command Line Interface installieren und konfigurieren. Weitere Informationen finden Sie im AWS Command Line Interface -Benutzerhandbuch.

So aktivieren Sie das Senden von E-Mails erneut

1. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den E-Mail-Versand für den Konfigurationssatz erneut zu aktivieren:

   ```
   aws ses update-configuration-set-sending-enabled \
   --configuration-set-name ConfigSet \
   --enabled
   ```

   Ersetzen Sie den Befehl im vorherigen Befehl *ConfigSet* durch den Namen des Konfigurationssatzes, für den Sie den E-Mail-Versand unterbrechen möchten.

2. Geben Sie in der Befehlszeile den folgenden Befehl ein, um sicherzustellen, dass das Senden von E-Mails aktiviert ist:

   ```
   aws ses describe-configuration-set \
   --configuration-set-name ConfigSet \
   --configuration-set-attribute-names reputationOptions
   ```

   Der Befehl erzeugt eine Ausgabe, die dem folgenden Beispiel ähnelt:

   ```
   {
       "ConfigurationSet": {
           "Name": "ConfigSet"
       },
       "ReputationOptions": {
           "ReputationMetricsEnabled": true,
           "SendingEnabled": true
       }
   }
   ```

   Wenn der `SendingEnabled`-Wert `true` lautet, dann wurde der E-Mail-Versand für den Konfigurationssatz erfolgreich neu aktiviert.

Teil 5: Erstellen eines Amazon-SNS-Themas

CloudWatch Um die Lambda-Funktion auszuführen, wenn ein Alarm ausgelöst wird, müssen Sie zunächst ein Amazon SNS SNS-Thema erstellen und die Lambda-Funktion abonnieren.

So erstellen Sie das Amazon-SNS-Thema

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie mithilfe der Regionsauswahl die Region aus, in der Sie den E-Mail-Versand automatisch pausieren möchten.
3. Wählen Sie im Navigationsbereich Topics (Themen) aus.
4. Wählen Sie Create new topic (Neues Thema erstellen).
5. Geben Sie im Fenster Create new topic (Neues Thema erstellen) unter Topic name (Themenname) einen Namen für das Thema ein. Optional können Sie im Feld Display name (Display-Name) einen aussagekräftigeren Namen eingeben.

   Wählen Sie Create topic (Thema erstellen) aus.
6. Aktivieren Sie in der Liste der Themen das Kontrollkästchen neben dem im vorherigen Schritt erstellten Thema. Wählen Sie im Menü Actions (Ereignis) die Option Subscribe to topic (Im Thema anmelden) aus.
7. Wählen Sie im Fenster Create subscription (Abonnement erstellen) folgende Optionen aus:
   - Für Protocol (Protokoll) wählen Sie AWS Lambda aus.
   - Wählen Sie für Endpoint (Endpunkt) die Lambda-Funktion aus, die Sie in the section called “Teil 3: Erstellen der Lambda-Funktion” erstellt haben.
   - Wählen Sie für Version or alias (Version oder alias) die Option default (Standard) aus.
8. Wählen Sie Create subscription (Abonnement erstellen) aus.

Teil 6: Einen Alarm erstellen CloudWatch

Dieser Abschnitt enthält Verfahren zum Erstellen eines Alarms CloudWatch , der ausgelöst wird, wenn eine Metrik einen bestimmten Schwellenwert erreicht. Wenn der Alarm ausgelöst wird, übermittelt er eine Benachrichtigung an das the section called “Teil 5: Erstellen eines Amazon-SNS-Themas”-Thema, das Sie in Amazon SNS erstellt haben, was dann wiederum die Lambda-Funktion auslöst, die Sie in the section called “Teil 3: Erstellen der Lambda-Funktion” erstellt haben.

Um einen CloudWatch Alarm zu erstellen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie mithilfe der Regionsauswahl die Region aus, in der Sie den E-Mail-Versand automatisch pausieren möchten.

3. Wählen Sie im Navigationsbereich auf der linken Seite Alarms (Alarme) aus.
4. Wählen Sie Alarm erstellen aus.
5. Wählen Sie im Fenster Create Alarm (Alarme erstellen) unter SES Metrics (SES-Metriken) die Option Configuration Set Metrics (Konfigurationsset-Metriken) aus.
6. Suchen Sie in der ses:configuration-set-Spalte den Konfigurationssatz, für den Sie einen Alarm erstellen möchten. Wählen Sie unter Metric Name (Metrikname) eine der folgenden Optionen aus:

   - Ruf. BounceRate — Wählen Sie diese Metrik, wenn Sie den E-Mail-Versand für den Konfigurationssatz unterbrechen möchten, wenn die allgemeine Hard-Bounce-Rate für den Konfigurationssatz einen von Ihnen definierten Schwellenwert überschreitet.
   - Ruf. ComplaintRate — Wählen Sie diese Metrik, wenn Sie den E-Mail-Versand für den Konfigurationssatz unterbrechen möchten, wenn die Gesamtbeschwerdequote für den Konfigurationssatz einen von Ihnen definierten Schwellenwert überschreitet.

   Wählen Sie Weiter aus.
7. Führen Sie folgende Schritte aus:

   - Geben Sie unter Alarm Threshold (Alarm-Schwellenwert) im Feld Name einen Namen für den Alarm ein.
   - Unter Wann auch immer: Ruf. BounceRateOder wann immer: Ruf. ComplaintRate, geben Sie den Schwellenwert an, durch den der Alarm ausgelöst wird.

     > **Note**
     >
     > Wenn die gesamte Unzustellbarkeitsquote für Ihr Amazon-SES-Konto 10 % überschreitet, oder wenn die gesamte Beschwerdequote für Ihr Amazon-SES-Konto 0,5 % überschreitet, wird für Ihr -Konto automatisch eine Prüfung festgelegt. Wenn Sie die Absprungs- oder Beschwerderate angeben, aufgrund derer der CloudWatch Alarm ausgelöst wird, empfehlen wir Ihnen, Werte zu verwenden, die weit unter diesen Raten liegen, um zu verhindern, dass Ihr Konto überprüft wird.

   - Wählen Sie unter Actions (Aktionen) für Whenever this alarm die Option State is ALARM (Status ist ALARM) aus. Wählen Sie für Send notification to (Benachrichtigung senden an) das Amazon-SNS-Thema aus, das Sie in the section called “Teil 5: Erstellen eines Amazon-SNS-Themas” erstellt haben.

Wählen Sie Alarm erstellen aus.

Teil 7: Testen der Lösung

Sie können jetzt den Alarm testen, um sicherzustellen, dass er die Lambda-Funktion ausführt, wenn er in den Status `ALARM` versetzt wird. Sie können den `SetAlarmState` Vorgang in der CloudWatch API verwenden, um den Status des Alarms vorübergehend zu ändern.

Die Verfahren in diesem Abschnitt sind optional, es wird jedoch empfohlen, diese durchzuführen, um zu überprüfen, ob die gesamte Lösung ordnungsgemäß konfiguriert ist.

So testen Sie die Lösung

1. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den Status des E-Mail-Versands für den Konfigurationssatz zu überprüfen:

   ```
   aws ses describe-configuration-set --configuration-set-name ConfigSet
   ```

   Wenn der Versand für den Konfigurationssatz aktiviert ist, wird die folgende Ausgabe angezeigt:

   ```
   {
       "ConfigurationSet": {
           "Name": "ConfigSet"
       },
       "ReputationOptions": {
           "ReputationMetricsEnabled": true,
           "SendingEnabled": true
       }
   }
   ```

   Wenn der `SendingEnabled`-Wert `true` lautet, dann ist der E-Mail-Versand für den Konfigurationssatz derzeit aktiviert.
2. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den Alarmstatus vorübergehend in `ALARM` zu ändern:

   ```
   aws cloudwatch set-alarm-state \
   --alarm-name MyAlarm \
   --state-value ALARM \
   ```

```
--state-reason "Testing execution of Lambda function"
```

Ersetzen Sie *MyAlarm* den vorherigen Befehl durch den Namen des Alarms, in dem Sie ihn erstellt habenthe section called “Teil 6: Einen Alarm erstellen CloudWatch”.

> **Note**
>
> Wenn Sie diesen Befehl ausführen, wechselt der Status des Alarms innerhalb weniger Sekunden von OK zu ALARM und zurück zu OK. Sie können diese Statusänderungen auf der Registerkarte Verlauf des Alarms in der CloudWatch Konsole oder mithilfe der DescribeAlarmHistoryOperation anzeigen.

3. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den Status des E-Mail-Versands für den Konfigurationssatz zu überprüfen:

```
aws ses describe-configuration-set \
--configuration-set-name ConfigSet
```

Wenn die Lambda-Funktion erfolgreich ausgeführt wird, sehen Sie eine Ausgabe, die dem folgenden Beispiel ähnelt:

```
{
    "ConfigurationSet": {
        "Name": "ConfigSet"
    },
    "ReputationOptions": {
        "ReputationMetricsEnabled": true,
        "SendingEnabled": false
    }
}
```

Wenn der `SendingEnabled`-Wert `false` lautet, dann ist das Senden von E-Mails für den Konfigurationssatz deaktiviert. Dies bedeutet, dass die Lambda-Funktion erfolgreich ausgeführt wurde.

4. Führen Sie die Schritte in the section called “Teil 4: Erneute Aktivierung des E-Mail-Versands für den Konfigurationssatz” aus, um den E-Mail-Versand für den Konfigurationssatz erneut zu aktivieren.

Überwachung von SES-Ereignissen mit Amazon EventBridge

EventBridge ist ein serverloser Dienst, der Ereignisse verwendet, um Anwendungskomponenten miteinander zu verbinden, sodass Sie leichter skalierbare, ereignisgesteuerte Anwendungen erstellen können. Bei der ereignisgesteuerten Architektur werden lose gekoppelte Softwaresysteme entwickelt, die zusammenarbeiten, indem sie Ereignisse senden und darauf reagieren. Bei Ereignissen handelt es sich um Nachrichten im JSON-Format, die in der Regel eine Änderung einer Ressource oder Umgebung oder ein anderes Verwaltungsereignis darstellen.

Bestimmte SES-Funktionen generieren Ereignisse, die Sie bei der Erstellung eines Ereignisziels definieren, und senden sie an den EventBridge Standard-Event-Bus. Ein Event Bus ist ein Router, der Ereignisse empfängt und sie an null oder mehr Ziele weiterleitet. Regeln, die Sie dem Event Bus zuordnen, werten die eintreffenden Ereignisse aus. Bei jeder Regel wird geprüft, ob ein Ereignis dem Muster der Regel entspricht. Wenn das Ereignis übereinstimmt, wird das Ereignis an die angegebenen Ziele EventBridge gesendet.

SES sendet Ereignisse, EventBridge wenn ein Feature einen Statuswechsel oder eine Statusaktualisierung erfährt. Sie können EventBridge Regeln verwenden, um Ereignisse an Ihre definierten Ziele weiterzuleiten. Diese Ereignisse werden auf Grundlage einer optimalen Leistung übermittelt und können in falscher Reihenfolge geliefert werden.

Themen

- SES-Ereignisse
- Referenz zu SES-Ereignisschemas
- Verwendung EventBridge mit SES-Ereignissen
- Zusätzliche EventBridge Ressourcen

SES-Ereignisse

Die folgenden Ereignisse werden von SES-Funktionen generiert und an den standardmäßigen Event-Bus-Eingang gesendet EventBridge. Weitere Informationen, einschließlich detaillierter Daten für jeden Ereignistyp, finden Sie unter???.

Veranstaltungen für Virtual Deliverability Manager-Berater

Ereignistyp	Description
Empfehlungsstatus des Beraters: Offen	Ein Ereignis, das immer dann generiert wird, wenn eine neue Empfehlung im Virtual-Deliverability-Manager-Berater geöffnet wird.
Empfehlungsstatus des Beraters: Gelöst	Ein Ereignis, das immer dann generiert wird, wenn eine Empfehlung im Virtual-Deliverability-Manager-Berater gelöst wird.

Ereignisse beim Senden von SES-E-Mails

Ereignistyp	Description
E-Mail wurde zurückgeschickt	Ein harter Bounce, bei dem der E-Mail-Server des Empfänger s die E-Mail dauerhaft zurückgewiesen hat. (Soft bounces (Temporäre Unzustellbarkeiten) werden nur dann aufgenomm en, wenn SES über einen bestimmten Zeitraum vergeblich versucht hat, die E-Mail zuzustellen.)
E-Mail angeklickt	Der Empfänger hat auf einen oder mehrere Links in der E-Mail geklickt.
E-Mail-Beschwerde erhalten	Die E-Mail wurde erfolgreich an den E-Mail-Server des Empfängers zugestellt, aber der Empfänger hat sie als Spam markiert.
E-Mail zugestellt	SES hat die E-Mail erfolgreich an den Mailserver des Empfänger s zugestellt.
E-Mail-Zustellung verzögert	Die E-Mail konnte nicht an den E-Mail-Server des Empfängers zugestellt werden, da ein vorübergehendes Problem aufgetret en ist. Verzögerungen bei der Zustellung können, z. B. auftreten , wenn der Posteingang des Empfängers voll ist oder der empfangende E-Mail-Server ein vorübergehendes Problem aufweist.

Ereignistyp	Description
E-Mail geöffnet	Der Empfänger hat die Nachricht erhalten und sie in seinem E-Mail-Client geöffnet.
E-Mail zurückgewiesen	SES akzeptierte die E-Mail, stellte jedoch fest, dass sie einen Virus enthielt, und versuchte nicht, sie an den E-Mail-Server des Empfängers zuzustellen.
Das Rendern der E-Mail ist fehlgeschlagen	Die E-Mail wurde aufgrund eines Problems beim Rendern der Vorlage nicht gesendet. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail-Vorlage mithilfe der `SendTemplatedEmail` - oder `SendBulkTemplatedEmail` -API-Operationen senden.
E-Mail gesendet	Die Sendeanfrage war erfolgreich und SES wird versuchen, die Nachricht an den Mailserver des Empfängers zu senden. (Wenn eine Unterdrückung auf Kontoebene oder eine globale Unterdrückung verwendet wird, zählt SES sie weiterhin als Senden, aber die Zustellung wird unterdrückt.)
E-Mail abonniert	Die E-Mail wurde erfolgreich zugestellt, aber der Empfänger hat die Abonnementeinstellungen aktualisiert, indem er `List-Unsubscribe` in den E-Mail-Header oder auf den `Unsubscribe` Link in der Fußzeile geklickt hat.

Referenz zu SES-Ereignisschemas

Alle Ereignisse von AWS Diensten haben einen gemeinsamen Satz von Feldern, die Metadaten über das Ereignis enthalten, z. B. den AWS Dienst, der die Quelle des Ereignisses ist, den Zeitpunkt, zu dem das Ereignis generiert wurde, das Konto und die Region, in der das Ereignis stattgefunden hat, und andere. Definitionen dieser allgemeinen Felder finden Sie unter Referenz zur Ereignisstruktur im EventBridge Benutzerhandbuch.

Darüber hinaus weist jedes Ereignis ein `detail`-Feld auf, das spezifische Daten für das betreffende Ereignis enthält. In der folgenden Referenz werden die Detailfelder für die verschiedenen SES-Ereignisse definiert.

Bei der EventBridge Auswahl und Verwaltung von SES-Ereignissen ist es hilfreich, Folgendes zu beachten:

- Das Feld `source` ist für alle Ereignisse aus SES auf `aws.ses` eingestellt.
- Das Feld `detail-type` gibt den Ereignistyp an. Die Tabelle mit den Ereignistypen finden Sie unterthe section called “SES-Ereignisse”.
- Das Feld `detail` enthält die Daten, die für das betreffende Ereignis spezifisch sind.

  Bei einigen Ereignistypen, z. B. denen für Virtual Deliverability Manager, ist das Detailfeld eine ziemlich vereinfachte Datenzeichenfolge, die aus einer endlichen Menge statischer Werte aufgefüllt wird. Umgekehrt ist das Detailfeld für E-Mail-Versandereignisse komplexer, da es aus vielen Detailunterfeldern bestehen kann, bei denen es sich um eine Kombination aus statischen und dynamischen Werten handelt, z. B. dem Zeitstempel, zu dem eine E-Mail gesendet wurde, der Empfängeradresse und vielen anderen E-Mail-Attributen.

Themen

- Schema des Status des Virtual-Deliverability-Manager-Beraters
- Statusschema für den SES-E-Mail-Versand

Schema des Status des Virtual-Deliverability-Manager-Beraters

Die folgende Schemareferenz definiert die Felder, die für Virtual Deliverability Manager-Beraterstatusereignisse spezifisch sind.

Definitionen für die allgemeinen Felder, die in allen Ereignisschemas vorkommen (wie`version`, `idaccount`, und andere), finden Sie in der Referenz zur Ereignisstruktur im EventBridge Benutzerhandbuch. Die Felder `source` und `detail-type` sind in der folgenden Referenz enthalten, da sie SES-spezifische Werte für SES-Ereignisse enthalten.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Bei SES-Ereignissen lautet dieser Wert `aws.ses`.

`detail-type`

Identifiziert den Ereignistyp.

Die Werte für dieses Feld sind in der Virtual Deliverability Manager-Advisor-Ereignistabelle unter aufgeführt. the section called “SES-Ereignisse”

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Die Werte für dieses Feld können sein:

- `DKIM verification is not enabled.`
- `DKIM verification has failed.`
- `DKIM signing key length is below 2048 bits.`
- `DMARC configuration was not found.`
- `DMARC configuration could not be parsed.`
- `DKIM record was not found.`
- `DKIM record is not aligned.`
- `MAIL FROM record is not aligned.`
- `SPF record was not found.`
- `SPF record for Amazon SES was not found.`
- `SPF all qualifier is missing.`
- `An SPF configuration issue was found.`
- `BIMI record not found or configured without default selector.`
- `BIMI has malformed TXT record.`

Example Beispiel: Statusereignis des Virtual-Deliverability-Manager-Beraters

Im Folgenden finden Sie ein Beispiel für ein Statusereignis des Virtual-Deliverability-Manager-Beraters für den Ereignistyp `Advisor Recommendation Status Open`. Der Detailereigniswert in diesem Beispiel ist`SPF record was not found.`.

```
{
 "version": "0",
  "id": "abcd9999-ef33-0123-90ab-abcdef666666",
```

```
  "detail-type": "Advisor Recommendation Status Open",
  "source": "aws.ses",
  "account": "012345678901",
  "time": "2023-11-15T17:00:59Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ses:us-east-1:012345678901:identity/vdm.events-publishing.cajun.syster-
games.example.com"
  ],
  "detail": { "version": "1.0.0", "data": "SPF record was not found." }
}
```

Statusschema für den SES-E-Mail-Versand

Die folgende Schemareferenz definiert die Felder, die für SES-E-Mail-Versandstatusereignisse spezifisch sind.

Definitionen für die allgemeinen Felder, die in allen Ereignisschemas vorkommen (wie`version`, `idaccount`, und andere), finden Sie in der Referenz zur Ereignisstruktur im EventBridge Benutzerhandbuch. Die Felder `source` und `detail-type` sind in der folgenden Referenz enthalten, da sie SES-spezifische Werte für SES-Ereignisse enthalten.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Bei SES-Ereignissen lautet dieser Wert `aws.ses`.

`detail-type`

Identifiziert den Ereignistyp.

Die Werte für dieses Feld sind in der Tabelle mit SES-E-Mail-Versandereignissen unter aufgeführtthe section called “SES-Ereignisse”.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Alle möglichen Werte für dieses Feld können hier nicht aufgeführt werden, da sie aus statischen und dynamischen Werten bestehen, die durch jede einzelne E-Mail generiert werden, die zu einem bestimmten Zeitpunkt gesendet wird. Es wird jedoch ein Beispiel bereitgestellt, um Ihnen eine Vorstellung davon zu geben, welche Art von Daten dieses Feld enthalten kann. Ausführliche

Beispieldaten für alle Ereignistypen beim Senden von E-Mails finden Sie in der EventBridge Sandbox, siehe[Geben Sie ein Beispielereignis an in EventBridge](#).

Ein Beispiel für Detaildaten, die für das SES-E-Mail-Versandereignis `Email Rendering Failed` generiert wurden:

```
...,
  "detail": {
    "eventType": "Rendering Failure",
    "mail": {
      "timestamp": "2018-01-22T18:43:06.197Z",
      "source": "sender@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "sendingAccountId": "123456789012",
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "destination": ["recipient@example.com"],
      "headersTruncated": false,
      "tags": {
        "ses:configuration-set": ["ConfigSet"]
      }
    },
    "failure": {
      "errorMessage": "Attribute 'attributeName' is not present in the rendering
 data.",
      "templateName": "MyTemplate"
    }
  }
```

Example Beispiel: Ereignis zum Status des E-Mail-Versands

Im Folgenden finden Sie ein Beispiel für das vollständige Ereignis mit dem Status des E-Mail-Versands für den Ereignistyp`Email Rendering Failed`. Der Detailereigniswert in diesem Beispiel ist eine Kombination aus statischen und dynamischen Werten, die auf dem E-Mail-Sendeereignis für eine bestimmte E-Mail basieren.

```
{
  "version": "0",
  "id": "12a18625-3328-fafd-2809-a5e16004f112",
  "detail-type": "Email Rendering Failed",
  "source": "aws.ses",
  "account": "123456789012",
```

```
  "time": "2023-07-17T16:48:05Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ses:us-east-1:123456789012:identity/example.com"],
  "detail": {
    "eventType": "Rendering Failure",
    "mail": {
      "timestamp": "2018-01-22T18:43:06.197Z",
      "source": "sender@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "sendingAccountId": "123456789012",
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "destination": ["recipient@example.com"],
      "headersTruncated": false,
      "tags": {
        "ses:configuration-set": ["ConfigSet"]
      }
    },
    "failure": {
      "errorMessage": "Attribute 'attributeName' is not present in the rendering
 data.",
      "templateName": "MyTemplate"
    }
  }
}
```

Verwendung EventBridge mit SES-Ereignissen

Standardmäßig sendet SES Ereignisse an den EventBridge Standard-Event-Bus. Sie können Regeln für den Standard-Event-Bus erstellen, um bestimmte Ereignisse zu identifizieren EventBridge , die an ein oder mehrere angegebene Ziele gesendet werden sollen. Jede Regel enthält ein Ereignismuster, das EventBridge verwendet wird, um Ereignisse zuzuordnen, sobald sie auf dem Event-Bus ankommen. Wenn ein Ereignis dem Ereignismuster für eine bestimmte Regel entspricht, wird das Ereignis an das in der Regel angegebene Ziel EventBridge gesendet.

In EventBridge ist die Definition eines Ereignismusters in der Regel Teil des umfassenderen Prozesses der Erstellung einer neuen Regel oder der Bearbeitung einer vorhandenen Regel. Informationen zum Erstellen von EventBridge Regeln finden Sie im EventBridge Benutzerhandbuch unter Erstellen von EventBridge Amazon-Regeln, die auf Ereignisse reagieren.

Mithilfe der Sandbox-Funktion unter können Sie schnell ein Ereignismuster definieren und anhand eines Beispielereignisses überprüfen, ob das Muster mit den gewünschten Ereignissen

übereinstimmt, ohne zuerst eine Regel erstellen oder bearbeiten zu müssen. EventBridge Ausführliche Anweisungen zur Verwendung der Sandbox finden Sie im Benutzerhandbuch unter Testen eines Ereignismusters mithilfe der EventBridge Sandbox. EventBridge

Geben Sie ein SES-Beispielereignis in der Sandbox an EventBridge

Sie können Beispielereignisse für SES-Ereignisse auswählen, um damit die erstellten Ereignismuster zu testen.

Um ein SES-Beispielereignis in der EventBridge Sandbox anzugeben

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Entwicklerressourcen und dann Sandbox aus. Wählen Sie auf der Seite Sandbox die Registerkarte Ereignismuster.
3. Wählen Sie als Quelle der Veranstaltung AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.
4. Wählen Sie im Bereich Beispielereignis für Typ des Beispielereignisses die Option AWS - Ereignisse aus.
5. Scrollen Sie für Beispielereignisse nach unten zu SES und wählen Sie dann das gewünschte SES-Ereignis aus.

   EventBridge zeigt ein Beispielereignis mit all seinen Detaildaten für den Ereignistyp an.

   Sie können dieses Ereignis dann verwenden, um das Ereignismuster zu testen, das Sie im Abschnitt Ereignismuster erstellen, oder es als Grundlage für die Erstellung eigener Beispielereignisse für Mustertests verwenden, die im folgenden Abschnitt behandelt werden.

Erstellen und Testen von Ereignismustern für SES-Ereignisse

Nachdem Sie, wie im vorherigen Abschnitt erklärt, ein Beispielereignis ausgewählt haben, können Sie ein Ereignismuster erstellen und anhand des Beispielereignisses sicherstellen, dass es den gewünschten Ereignissen entspricht.

Um ein Ereignismuster zu erstellen und zu testen, das den SES-Ereignissen in der EventBridge Sandbox entspricht

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.

2. Wählen Sie im Navigationsbereich Entwicklerressourcen und dann Sandbox aus. Wählen Sie auf der Seite Sandbox die Registerkarte Ereignismuster.
3. Wählen Sie als Ereignisquelle AWS Ereignisse oder EventBridge Partnerereignisse aus und wählen Sie das Beispielereignis aus, das Sie testen möchten, wie im vorherigen Abschnitt beschrieben.
4. Scrollen Sie nach unten zu Erstellungsmethode und wählen Sie Musterformular verwenden aus.
5. Wählen Sie im Bereich Ereignismuster unter Ereignisquelle die Option AWS -Services aus.
6. Wählen Sie unter AWS Service die Option SES aus.
7. Wählen Sie unter Ereignistyp den SES-Ereignistyp aus, den Sie zuordnen möchten.

   EventBridge zeigt das minimale Ereignismuster, bestehend aus `detail-type` Feldern `source` und, an, das dem ausgewählten SES-Ereignis entspricht.

   In den beiden Beispielen entspricht das erste Ereignismuster allen `Advisor Recommendation Status Resolved` Ereignissen und im zweiten allen `Email Bounced` Ereignissen:

   ```
   {
     "source": ["aws.ses"],
     "detail-type": ["Advisor Recommendation Status Resolved"]
   }
   ```

   ```
   {
     "source": ["aws.ses"],
     "detail-type": ["Email Bounced"]
   }
   ```

8. Um Änderungen am Ereignismuster vorzunehmen, wählen Sie Muster bearbeiten aus und nehmen Sie Ihre Änderungen im JSON-Editor vor.

   Außerdem kann die Zuordnung auf Grundlage von Werten in einem oder mehreren Feldern mit Detaildaten erfolgen. Dazu gehört die Angabe mehrerer möglicher Werte für einen Feldwert.

   Im folgenden Beispiel wurde das Detailfeld zum generierten Mindestereignismuster hinzugefügt, wobei der `data` Feldwert als `DKIM record was not found` angegeben wurde, um alle Virtual Deliverability Manager-Advisor-Ereignisse mit demselben Detailwert zu finden:

   ```
   {
     "source": ["aws.ses"],
   ```

```
  "detail-type": ["Advisor Recommendation Status Resolved"],
  "detail": {
    "data": ["DKIM record was not found."]
  }
}
```

In diesem Beispiel wurden Detail-Unterfelder hinzugefügt, um über Ereignisse zu berichten, die durch alle E-Mails generiert wurden, die von noreply@example.com am 05.08.2024 gesendet und zurückgesendet wurden. (Der Präfixabgleich wird hier als Teil der Inhaltsfilterung verwendet.):

```
{
  "source": ["aws.ses"],
  "detail-type": ["Email Bounced"],
  "detail": {
    "mail": {
      "timestamp": [{
        "prefix": "2024-08-05"
      }],
      "source": ["noreply@example.com"]
    }
  }
}
```

Es ist wichtig, dass Sie den Abschnitt Ereignismuster im EventBridge Benutzerhandbuch lesen. Dort wird erklärt, dass der Wert für das Ereignismuster, den Sie in den JSON-Editor eingeben, von eckigen Klammern umgeben sein muss`[...]`, da er als Array betrachtet wird. Diese und weitere Informationen zur Erstellung erweiterter Ereignismuster finden Sie ebenfalls.

9. Um zu testen, ob Ihr Ereignismuster mit dem Beispielereignis übereinstimmt, das Sie oben im Bereich Beispielereignis angegeben haben, wählen Sie Testmuster aus. Wenn es übereinstimmt, wird unten im JSON-Editor ein grünes Banner mit der Aufschrift „Das Beispielereignis stimmte mit dem Ereignismuster überein“ angezeigt.
10. So beheben Sie Fehler nach der Auswahl von Testmuster:

    - Wenn es JSON-bezogene Fehler gibt, wird in der Meldung der Grund angegeben, z. B. „Das Ereignismuster ist nicht gültig. Grund: „Daten“ müssen ein Objekt oder ein Array in Zeile: 5, Spalte: 14 sein.“ Um dem abzuhelfen, schließen Sie den Wert in Zeile 5 mit eckigen Klammern ein. `[...]`

- Wenn es eine Diskrepanz zwischen den Werten im Beispielereignis und Ihrem Ereignismuster gibt, wird die Meldung „Das Beispielereignis stimmte nicht mit dem Ereignismuster überein“ angezeigt. Das bedeutet, dass sich ein oder mehrere Werte, die Sie testen möchten, von den Beispielwerten unterscheiden, die vom Generator für Beispielereignisse generiert wurden. Um dieses Problem zu beheben, fahren Sie mit den verbleibenden Schritten fort.

11. Um die Beispielwerte im Beispielereignis zu ändern, um Ihr Event-Muster erfolgreich zu testen, wählen Sie im Bereich Beispielereignis im JSON-Editor die Option Kopieren aus.
12. Wählen Sie über dem Editor das Optionsfeld neben Eigenen eingeben für den Ereignistyp Beispiel aus.
13. Fügen Sie das Beispielereignis in den JSON-Editor ein, und ersetzen Sie für jedes Feld, das Sie in Ihrem Ereignismuster verwenden, den Wert desselben Felds so, dass er dem Wert entspricht, den Sie in Ihrem Ereignismuster angegeben haben.
14. Scrollen Sie zurück zum Bereich Ereignismuster und wählen Sie erneut Muster testen aus. Wenn alle Werte korrekt eingegeben wurden und übereinstimmen, wird unten im JSON-Editor ein grünes Banner mit der Aufschrift „Das Beispielereignis stimmte mit dem Ereignismuster überein“ angezeigt.

Zusätzliche EventBridge Ressourcen

Weitere Informationen zur Verarbeitung und Verwaltung von Ereignissen finden Sie EventBridge in den folgenden Themen im EventBridge Amazon-Benutzerhandbuch.

- Detaillierte Informationen zur Funktionsweise von Eventbussen finden Sie unter Amazon EventBridge Event Bus.
- Informationen zur Ereignisstruktur finden Sie unter Ereignisse
- Informationen zur Erstellung von Ereignismustern, die beim EventBridge Abgleich von Ereignissen mit Regeln verwendet werden können, finden Sie unter Ereignismuster
- Informationen zum Erstellen von Regeln, mit denen angegeben wird, welche Ereignisse EventBridge verarbeitet werden, finden Sie unter Regeln
- Informationen zur Angabe, an welche Dienste oder andere Ziele EventBridge übereinstimmende Ereignisse senden, finden Sie unter Ziele

Codebeispiele für Amazon SES mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Amazon SES mit einem AWS Software Development Kit (SDK) verwendet wird.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele

- Codebeispiele für Amazon SES mit AWS SDKs
  - Grundlegende Beispiele für die Verwendung von Amazon SES AWS SDKs
    - Aktionen für Amazon SES mit AWS SDKs
      - Verwenden Sie es CreateReceiptFilter mit einem AWS SDK
      - CreateReceiptRuleMit einem AWS SDK verwenden
      - CreateReceiptRuleSetMit einem AWS SDK verwenden
      - CreateTemplateMit einem AWS SDK verwenden
      - Verwendung DeleteIdentity mit einem AWS SDK oder CLI
      - DeleteReceiptFilterMit einem AWS SDK verwenden
      - DeleteReceiptRuleMit einem AWS SDK verwenden
      - DeleteReceiptRuleSetMit einem AWS SDK verwenden
      - DeleteTemplateMit einem AWS SDK verwenden
      - DescribeReceiptRuleSetMit einem AWS SDK verwenden
      - Verwendung GetIdentityVerificationAttributes mit einem AWS SDK oder CLI
      - Verwendung GetSendQuota mit einem AWS SDK oder CLI
      - Verwendung von GetSendStatistics mit einer CLI
      - GetTemplateMit einem AWS SDK verwenden
      - Verwendung ListIdentities mit einem AWS SDK oder CLI
      - ListReceiptFiltersMit einem AWS SDK verwenden
      - ListTemplatesMit einem AWS SDK verwenden
      - SendBulkTemplatedEmailMit einem AWS SDK verwenden
      - Verwendung SendEmail mit einem AWS SDK oder CLI

        - Verwendung SendRawEmail mit einem AWS SDK oder CLI
        - SendTemplatedEmailMit einem AWS SDK verwenden
        - UpdateTemplateMit einem AWS SDK verwenden
        - Verwendung VerifyDomainIdentity mit einem AWS SDK oder CLI
        - Verwendung VerifyEmailIdentity mit einem AWS SDK oder CLI
    - Szenarien für die Verwendung von Amazon SES AWS SDKs
        - Erstellen einer Amazon-Transcribe-Streaming-App
        - Kopieren Sie Amazon SES SES-E-Mail- und Domainidentitäten mithilfe eines AWS SDK von einer Region in eine AWS andere
        - Erstellen einer Webanwendung zur Verfolgung von DynamoDB-Daten
        - Erstellen eines Amazon-Redshift-Element-Trackers
        - Erstellen eines Trackers für Aurora-Serverless-Arbeitsaufgaben
        - Ermitteln Sie persönliche Schutzausrüstung in Bildern mit Amazon Rekognition mithilfe eines SDK AWS
        - Objekte in Bildern mit Amazon Rekognition mithilfe eines SDK erkennen AWS
        - Erkennen Sie Personen und Objekte in einem Video mit Amazon Rekognition mithilfe eines SDK AWS
        - Generieren von Anmeldeinformationen für die Verbindung mit einem Amazon-SES-SMTP-Endpunkt
        - Amazon Simple Email Service (SES) einrichten
        - Verwenden von Step Functions, um Lambda-Funktionen aufzurufen
        - Überprüfen Sie eine E-Mail-Identität und senden Sie Nachrichten mit Amazon SES mithilfe eines AWS SDK
- Codebeispiele für Amazon SES API v2 mit AWS SDKs
    - Grundlegende Beispiele für die Verwendung von Amazon SES API v2 AWS SDKs
        - Aktionen für Amazon SES API v2 mit AWS SDKs
            - Verwenden Sie es CreateContact mit einem AWS SDK
            - CreateContactListMit einem AWS SDK verwenden
            - CreateEmailIdentityMit einem AWS SDK verwenden
            - CreateEmailTemplateMit einem AWS SDK verwenden
            - DeleteContactListMit einem AWS SDK verwenden

        - DeleteEmailIdentityMit einem AWS SDK verwenden
        - DeleteEmailTemplateMit einem AWS SDK verwenden
        - GetEmailIdentityMit einem AWS SDK verwenden
        - ListContactListsMit einem AWS SDK verwenden
        - ListContactsMit einem AWS SDK verwenden
        - SendEmailMit einem AWS SDK verwenden
- Szenarien für die Verwendung von Amazon SES API v2 AWS SDKs
    - Ein vollständiges Amazon SES API v2-Newsletter-Szenario mit einem AWS SDK

Codebeispiele für Amazon SES mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Amazon SES mit einem AWS Software Development Kit (SDK) verwendet wird.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Service-Funktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien anzeigen.

Szenarien sind Codebeispiele, die Ihnen zeigen, wie Sie bestimmte Aufgaben ausführen, indem Sie mehrere Funktionen innerhalb eines Service aufrufen oder mit anderen AWS-Services kombinieren.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Amazon SES

- Grundlegende Beispiele für die Verwendung von Amazon SES AWS SDKs
    - Aktionen für Amazon SES mit AWS SDKs
        - Verwenden Sie es CreateReceiptFilter mit einem AWS SDK
        - CreateReceiptRuleMit einem AWS SDK verwenden
        - CreateReceiptRuleSetMit einem AWS SDK verwenden
        - CreateTemplateMit einem AWS SDK verwenden
        - Verwendung DeleteIdentity mit einem AWS SDK oder CLI
        - DeleteReceiptFilterMit einem AWS SDK verwenden

- DeleteReceiptRuleMit einem AWS SDK verwenden
- DeleteReceiptRuleSetMit einem AWS SDK verwenden
- DeleteTemplateMit einem AWS SDK verwenden
- DescribeReceiptRuleSetMit einem AWS SDK verwenden
- Verwendung GetIdentityVerificationAttributes mit einem AWS SDK oder CLI
- Verwendung GetSendQuota mit einem AWS SDK oder CLI
- Verwendung von GetSendStatistics mit einer CLI
- GetTemplateMit einem AWS SDK verwenden
- Verwendung ListIdentities mit einem AWS SDK oder CLI
- ListReceiptFiltersMit einem AWS SDK verwenden
- ListTemplatesMit einem AWS SDK verwenden
- SendBulkTemplatedEmailMit einem AWS SDK verwenden
- Verwendung SendEmail mit einem AWS SDK oder CLI
- Verwendung SendRawEmail mit einem AWS SDK oder CLI
- SendTemplatedEmailMit einem AWS SDK verwenden
- UpdateTemplateMit einem AWS SDK verwenden
- Verwendung VerifyDomainIdentity mit einem AWS SDK oder CLI
- Verwendung VerifyEmailIdentity mit einem AWS SDK oder CLI

- Szenarien für die Verwendung von Amazon SES AWS SDKs
  - Erstellen einer Amazon-Transcribe-Streaming-App
  - Kopieren Sie Amazon SES SES-E-Mail- und Domainidentitäten mithilfe eines AWS SDK von einer Region in eine AWS andere
  - Erstellen einer Webanwendung zur Verfolgung von DynamoDB-Daten
  - Erstellen eines Amazon-Redshift-Element-Trackers
  - Erstellen eines Trackers für Aurora-Serverless-Arbeitsaufgaben
  - Ermitteln Sie persönliche Schutzausrüstung in Bildern mit Amazon Rekognition mithilfe eines SDK AWS
  - Objekte in Bildern mit Amazon Rekognition mithilfe eines SDK erkennen AWS
  - Erkennen Sie Personen und Objekte in einem Video mit Amazon Rekognition mithilfe eines SDK AWS

- Generieren von Anmeldeinformationen für die Verbindung mit einem Amazon-SES-SMTP-Endpunkt
- Amazon Simple Email Service (SES) einrichten
- Verwenden von Step Functions, um Lambda-Funktionen aufzurufen
- Überprüfen Sie eine E-Mail-Identität und senden Sie Nachrichten mit Amazon SES mithilfe eines AWS SDK

Grundlegende Beispiele für die Verwendung von Amazon SES AWS SDKs

Die folgenden Codebeispiele zeigen, wie Sie die Grundlagen von Amazon Simple Email Service mit verwenden können AWS SDKs.

Beispiele

- Aktionen für Amazon SES mit AWS SDKs
  - Verwenden Sie es CreateReceiptFilter mit einem AWS SDK
  - CreateReceiptRuleMit einem AWS SDK verwenden
  - CreateReceiptRuleSetMit einem AWS SDK verwenden
  - CreateTemplateMit einem AWS SDK verwenden
  - Verwendung DeleteIdentity mit einem AWS SDK oder CLI
  - DeleteReceiptFilterMit einem AWS SDK verwenden
  - DeleteReceiptRuleMit einem AWS SDK verwenden
  - DeleteReceiptRuleSetMit einem AWS SDK verwenden
  - DeleteTemplateMit einem AWS SDK verwenden
  - DescribeReceiptRuleSetMit einem AWS SDK verwenden
  - Verwendung GetIdentityVerificationAttributes mit einem AWS SDK oder CLI
  - Verwendung GetSendQuota mit einem AWS SDK oder CLI
  - Verwendung von GetSendStatistics mit einer CLI
  - GetTemplateMit einem AWS SDK verwenden
  - Verwendung ListIdentities mit einem AWS SDK oder CLI
  - ListReceiptFiltersMit einem AWS SDK verwenden
  - ListTemplatesMit einem AWS SDK verwenden
  - SendBulkTemplatedEmailMit einem AWS SDK verwenden

- Verwendung SendEmail mit einem AWS SDK oder CLI
- Verwendung SendRawEmail mit einem AWS SDK oder CLI
- SendTemplatedEmailMit einem AWS SDK verwenden
- UpdateTemplateMit einem AWS SDK verwenden
- Verwendung VerifyDomainIdentity mit einem AWS SDK oder CLI
- Verwendung VerifyEmailIdentity mit einem AWS SDK oder CLI

Aktionen für Amazon SES mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Sie einzelne Amazon SES SES-Aktionen mit ausführen AWS SDKs. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden können.

Diese Auszüge rufen die Amazon–SES-API auf und sind Codeauszüge aus größeren Programmen, die im Kontext ausgeführt werden müssen. Sie können Aktionen im Kontext unter Szenarien für die Verwendung von Amazon SES AWS SDKs anzeigen.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der API-Referenz zu Amazon Simple Email Service.

Beispiele

- Verwenden Sie es CreateReceiptFilter mit einem AWS SDK
- CreateReceiptRuleMit einem AWS SDK verwenden
- CreateReceiptRuleSetMit einem AWS SDK verwenden
- CreateTemplateMit einem AWS SDK verwenden
- Verwendung DeleteIdentity mit einem AWS SDK oder CLI
- DeleteReceiptFilterMit einem AWS SDK verwenden
- DeleteReceiptRuleMit einem AWS SDK verwenden
- DeleteReceiptRuleSetMit einem AWS SDK verwenden
- DeleteTemplateMit einem AWS SDK verwenden
- DescribeReceiptRuleSetMit einem AWS SDK verwenden
- Verwendung GetIdentityVerificationAttributes mit einem AWS SDK oder CLI
- Verwendung GetSendQuota mit einem AWS SDK oder CLI
- Verwendung von GetSendStatistics mit einer CLI

- GetTemplateMit einem AWS SDK verwenden
- Verwendung ListIdentities mit einem AWS SDK oder CLI
- ListReceiptFiltersMit einem AWS SDK verwenden
- ListTemplatesMit einem AWS SDK verwenden
- SendBulkTemplatedEmailMit einem AWS SDK verwenden
- Verwendung SendEmail mit einem AWS SDK oder CLI
- Verwendung SendRawEmail mit einem AWS SDK oder CLI
- SendTemplatedEmailMit einem AWS SDK verwenden
- UpdateTemplateMit einem AWS SDK verwenden
- Verwendung VerifyDomainIdentity mit einem AWS SDK oder CLI
- Verwendung VerifyEmailIdentity mit einem AWS SDK oder CLI

Verwenden Sie es **`CreateReceiptFilter`** mit einem AWS SDK

Die folgenden Code-Beispiele zeigen, wie `CreateReceiptFilter` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Create an Amazon Simple Email Service (Amazon SES) receipt filter..
/*!
  \param receiptFilterName: The name for the receipt filter.
  \param cidr: IP address or IP address range in Classless Inter-Domain Routing
 (CIDR) notation.
  \param policy: Block or allow enum of type ReceiptFilterPolicy.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::createReceiptFilter(const Aws::String &receiptFilterName,
                                      const Aws::String &cidr,
```

```
                                        Aws::SES::Model::ReceiptFilterPolicy
 policy,
                                        const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);
    Aws::SES::Model::CreateReceiptFilterRequest createReceiptFilterRequest;
    Aws::SES::Model::ReceiptFilter receiptFilter;
    Aws::SES::Model::ReceiptIpFilter receiptIpFilter;
    receiptIpFilter.SetCidr(cidr);
    receiptIpFilter.SetPolicy(policy);
    receiptFilter.SetName(receiptFilterName);
    receiptFilter.SetIpFilter(receiptIpFilter);
    createReceiptFilterRequest.SetFilter(receiptFilter);
    Aws::SES::Model::CreateReceiptFilterOutcome createReceiptFilterOutcome =
 sesClient.CreateReceiptFilter(
            createReceiptFilterRequest);
    if (createReceiptFilterOutcome.IsSuccess()) {
        std::cout << "Successfully created receipt filter." << std::endl;
    }
    else {
        std::cerr << "Error creating receipt filter: " <<
                  createReceiptFilterOutcome.GetError().GetMessage() <<
 std::endl;
    }

    return createReceiptFilterOutcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateReceiptFilterin der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import {
```

```
  CreateReceiptFilterCommand,
  ReceiptFilterPolicy,
} from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const createCreateReceiptFilterCommand = ({ policy, ipOrRange, name }) => {
  return new CreateReceiptFilterCommand({
    Filter: {
      IpFilter: {
        Cidr: ipOrRange, // string, either a single IP address (10.0.0.1) or an
 IP address range in CIDR notation (10.0.0.1/24)).
        Policy: policy, // enum ReceiptFilterPolicy, email traffic from the
 filtered addressesOptions.
      },
      /*
        The name of the IP address filter. Only ASCII letters, numbers,
 underscores, or dashes.
        Must be less than 64 characters and start and end with a letter or
 number.
       */
      Name: name,
    },
  });
};

const FILTER_NAME = getUniqueName("ReceiptFilter");

const run = async () => {
  const createReceiptFilterCommand = createCreateReceiptFilterCommand({
    policy: ReceiptFilterPolicy.Allow,
    ipOrRange: "10.0.0.1",
    name: FILTER_NAME,
  });

  try {
    return await sesClient.send(createReceiptFilterCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
```

```
  }
};
```

- Einzelheiten zur API finden Sie CreateReceiptFilterin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def create_receipt_filter(self, filter_name, ip_address_or_range, allow):
        """
        Creates a filter that allows or blocks incoming mail from an IP address
 or
        range.

        :param filter_name: The name to give the filter.
        :param ip_address_or_range: The IP address or range to block or allow.
        :param allow: When True, incoming mail is allowed from the specified IP
                      address or range; otherwise, it is blocked.
        """
```

```
        try:
            policy = "Allow" if allow else "Block"
            self.ses_client.create_receipt_filter(
                Filter={
                    "Name": filter_name,
                    "IpFilter": {"Cidr": ip_address_or_range, "Policy": policy},
                }
            )
            logger.info(
                "Created receipt filter %s to %s IP of %s.",
                filter_name,
                policy,
                ip_address_or_range,
            )
        except ClientError:
            logger.exception("Couldn't create receipt filter %s.", filter_name)
            raise
```

- Einzelheiten zur API finden Sie CreateReceiptFilterin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
" iv_allow = abap_true means 'Allow', abap_false means 'Block'
DATA(lv_policy) = COND /aws1/sesreceiptfilterpolicy(
  WHEN iv_allow = abap_true THEN 'Allow'
  ELSE 'Block'
).

DATA(lo_ip_filter) = NEW /aws1/cl_sesreceiptipfilter(
  iv_policy = lv_policy
```

```
      iv_cidr = iv_ip_address_or_range
    ).

    DATA(lo_filter) = NEW /aws1/cl_sesreceiptfilter(
      iv_name = iv_filter_name
      io_ipfilter = lo_ip_filter
    ).

    TRY.
        lo_ses->createreceiptfilter( io_filter = lo_filter ).
        MESSAGE 'Receipt filter created successfully' TYPE 'I'.
      CATCH /aws1/cx_sesalreadyexistsex INTO DATA(lo_ex1).
        DATA(lv_error) = |Filter already exists: { lo_ex1->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex1.
      CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
        lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex_generic.
    ENDTRY.
```

- Einzelheiten zur API finden Sie CreateReceiptFilterin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`CreateReceiptRule`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `CreateReceiptRule` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Create an Amazon Simple Email Service (Amazon SES) receipt rule.
/*!
  \param receiptRuleName: The name for the receipt rule.
  \param s3BucketName: The name of the S3 bucket for incoming mail.
  \param s3ObjectKeyPrefix: The prefix for the objects in the S3 bucket.
  \param ruleSetName: The name of the rule set where the receipt rule is added.
  \param recipients: Aws::Vector of recipients.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::createReceiptRule(const Aws::String &receiptRuleName,
                                    const Aws::String &s3BucketName,
                                    const Aws::String &s3ObjectKeyPrefix,
                                    const Aws::String &ruleSetName,
                                    const Aws::Vector<Aws::String> &recipients,
                                    const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::CreateReceiptRuleRequest createReceiptRuleRequest;

    Aws::SES::Model::S3Action s3Action;
    s3Action.SetBucketName(s3BucketName);
    s3Action.SetObjectKeyPrefix(s3ObjectKeyPrefix);

    Aws::SES::Model::ReceiptAction receiptAction;
    receiptAction.SetS3Action(s3Action);

    Aws::SES::Model::ReceiptRule receiptRule;
    receiptRule.SetName(receiptRuleName);
    receiptRule.WithRecipients(recipients);

    Aws::Vector<Aws::SES::Model::ReceiptAction> receiptActionList;
    receiptActionList.emplace_back(receiptAction);
    receiptRule.SetActions(receiptActionList);

    createReceiptRuleRequest.SetRuleSetName(ruleSetName);
    createReceiptRuleRequest.SetRule(receiptRule);

    auto outcome = sesClient.CreateReceiptRule(createReceiptRuleRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully created receipt rule." << std::endl;
```

```
    }
    else {
        std::cerr << "Error creating receipt rule. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateReceiptRulein der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { CreateReceiptRuleCommand, TlsPolicy } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const RULE_SET_NAME = getUniqueName("RuleSetName");
const RULE_NAME = getUniqueName("RuleName");
const S3_BUCKET_NAME = getUniqueName("S3BucketName");

const createS3ReceiptRuleCommand = ({
  bucketName,
  emailAddresses,
  name,
  ruleSet,
}) => {
  return new CreateReceiptRuleCommand({
    Rule: {
      Actions: [
        {
```

```
          S3Action: {
            BucketName: bucketName,
            ObjectKeyPrefix: "email",
          },
        },
      ],
      Recipients: emailAddresses,
      Enabled: true,
      Name: name,
      ScanEnabled: false,
      TlsPolicy: TlsPolicy.Optional,
    },
    RuleSetName: ruleSet, // Required
  });
};

const run = async () => {
  const s3ReceiptRuleCommand = createS3ReceiptRuleCommand({
    bucketName: S3_BUCKET_NAME,
    emailAddresses: ["email@example.com"],
    name: RULE_NAME,
    ruleSet: RULE_SET_NAME,
  });

  try {
    return await sesClient.send(s3ReceiptRuleCommand);
  } catch (err) {
    console.log("Failed to create S3 receipt rule.", err);
    throw err;
  }
};
```

- Einzelheiten zur API finden Sie CreateReceiptRulein der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie einen Amazon-S3-Bucket, in dem Amazon SES Kopien eingehender E-Mails ablegen und eine Regel erstellen kann, die eingehende E-Mails für eine bestimmte Empfängerliste in den Bucket kopiert.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def create_bucket_for_copy(self, bucket_name):
        """
        Creates a bucket that can receive copies of emails from Amazon SES. This
        includes adding a policy to the bucket that grants Amazon SES permission
        to put objects in the bucket.

        :param bucket_name: The name of the bucket to create.
        :return: The newly created bucket.
        """
        allow_ses_put_policy = {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "AllowSESPut",
                    "Effect": "Allow",
                    "Principal": {"Service": "ses.amazonaws.com"},
```

```
                    "Action": "s3:PutObject",
                    "Resource": f"arn:aws:s3:::{bucket_name}/*",
                }
            ],
        }
        bucket = None
        try:
            bucket = self.s3_resource.create_bucket(
                Bucket=bucket_name,
                CreateBucketConfiguration={
                    "LocationConstraint":
self.s3_resource.meta.client.meta.region_name
                },
            )
            bucket.wait_until_exists()
            bucket.Policy().put(Policy=json.dumps(allow_ses_put_policy))
            logger.info("Created bucket %s to receive copies of emails.",
bucket_name)
        except ClientError:
            logger.exception("Couldn't create bucket to receive copies of
emails.")
            if bucket is not None:
                bucket.delete()
            raise
        else:
            return bucket


    def create_s3_copy_rule(
        self, rule_set_name, rule_name, recipients, bucket_name, prefix
    ):
        """
        Creates a rule so that all emails received by the specified recipients
are
        copied to an Amazon S3 bucket.

        :param rule_set_name: The name of a previously created rule set to
contain
                              this rule.
        :param rule_name: The name to give the rule.
        :param recipients: When an email is received by one of these recipients,
it
                           is copied to the Amazon S3 bucket.
        :param bucket_name: The name of the bucket to receive email copies. This
```

```
                            bucket must allow Amazon SES to put objects into it.
        :param prefix: An object key prefix to give the emails copied to the
bucket.
        """
        try:
            self.ses_client.create_receipt_rule(
                RuleSetName=rule_set_name,
                Rule={
                    "Name": rule_name,
                    "Enabled": True,
                    "Recipients": recipients,
                    "Actions": [
                        {
                            "S3Action": {
                                "BucketName": bucket_name,
                                "ObjectKeyPrefix": prefix,
                            }
                        }
                    ],
                },
            )
            logger.info(
                "Created rule %s to copy mail received by %s to bucket %s.",
                rule_name,
                recipients,
                bucket_name,
            )
        except ClientError:
            logger.exception("Couldn't create rule %s.", rule_name)
            raise
```

- Einzelheiten zur API finden Sie CreateReceiptRulein AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
" Create S3 action for copying emails to S3
DATA(lo_s3_action) = NEW /aws1/cl_sess3action(
  iv_bucketname = iv_bucket_name
  iv_objectkeyprefix = iv_prefix
).

" Create receipt action with S3 action
DATA(lo_action) = NEW /aws1/cl_sesreceiptaction(
  io_s3action = lo_s3_action
).

" Create list of actions
DATA lt_actions TYPE /aws1/cl_sesreceiptaction=>tt_receiptactionslist.
APPEND lo_action TO lt_actions.

" Create receipt rule
DATA(lo_rule) = NEW /aws1/cl_sesreceiptrule(
  iv_name = iv_rule_name
  iv_enabled = abap_true
  it_recipients = it_recipients
  it_actions = lt_actions
).

TRY.
    lo_ses->createreceiptrule(
      iv_rulesetname = iv_rule_set_name
      io_rule = lo_rule
    ).
    MESSAGE 'Receipt rule created successfully' TYPE 'I'.
  CATCH /aws1/cx_sesinvalids3confex INTO DATA(lo_ex1).
    DATA(lv_error) = |Invalid S3 configuration: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
```

```
        RAISE EXCEPTION lo_ex1.
      CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
        lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex_generic.
    ENDTRY.
```

- Einzelheiten zur API finden Sie CreateReceiptRulein der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`CreateReceiptRuleSet`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `CreateReceiptRuleSet` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Create an Amazon Simple Email Service (Amazon SES) receipt rule set.
/*!
  \param ruleSetName: The name of the rule set.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::createReceiptRuleSet(const Aws::String &ruleSetName,
                                       const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::CreateReceiptRuleSetRequest createReceiptRuleSetRequest;
```

```
    createReceiptRuleSetRequest.SetRuleSetName(ruleSetName);

    Aws::SES::Model::CreateReceiptRuleSetOutcome outcome =
 sesClient.CreateReceiptRuleSet(
           createReceiptRuleSetRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully created receipt rule set." << std::endl;
    }
    else {
        std::cerr << "Error creating receipt rule set. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateReceiptRuleSetin der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { CreateReceiptRuleSetCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const RULE_SET_NAME = getUniqueName("RuleSetName");

const createCreateReceiptRuleSetCommand = (ruleSetName) => {
  return new CreateReceiptRuleSetCommand({ RuleSetName: ruleSetName });
```

```
};

const run = async () => {
  const createReceiptRuleSetCommand =
    createCreateReceiptRuleSetCommand(RULE_SET_NAME);

  try {
    return await sesClient.send(createReceiptRuleSetCommand);
  } catch (err) {
    console.log("Failed to create receipt rule set", err);
    return err;
  }
};
```

- Einzelheiten zur API finden Sie CreateReceiptRuleSetin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def create_receipt_rule_set(self, rule_set_name):
```

```
        """
        Creates an empty rule set. Rule sets contain individual rules and can be
        used to organize rules.

        :param rule_set_name: The name to give the rule set.
        """
        try:
            self.ses_client.create_receipt_rule_set(RuleSetName=rule_set_name)
            logger.info("Created receipt rule set %s.", rule_set_name)
        except ClientError:
            logger.exception("Couldn't create receipt rule set %s.",
rule_set_name)
            raise
```

- Einzelheiten zur API finden Sie CreateReceiptRuleSetin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    TRY.
        lo_ses->createreceiptruleset( iv_rulesetname = iv_rule_set_name ).
        MESSAGE 'Receipt rule set created successfully' TYPE 'I'.
      CATCH /aws1/cx_sesalreadyexistsex INTO DATA(lo_ex1).
        DATA(lv_error) = |Rule set already exists: { lo_ex1->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex1.
      CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
        lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex_generic.
    ENDTRY.
```

- Einzelheiten zur API finden Sie CreateReceiptRuleSetin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`CreateTemplate`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `CreateTemplate` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Create an email template.
    /// </summary>
    /// <param name="name">Name of the template.</param>
    /// <param name="subject">Email subject.</param>
    /// <param name="text">Email body text.</param>
    /// <param name="html">Email HTML body text.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateEmailTemplateAsync(string name, string subject,
string text,
        string html)
```

```
    {
        var success = false;
        try
        {
            var response = await _amazonSimpleEmailService.CreateTemplateAsync(
                new CreateTemplateRequest
                {
                    Template = new Template
                    {
                        TemplateName = name,
                        SubjectPart = subject,
                        TextPart = text,
                        HtmlPart = html
                    }
                });
            success = response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Exception ex)
        {
            Console.WriteLine("CreateEmailTemplateAsync failed with exception: "
+ ex.Message);
        }

        return success;
    }
```

- Einzelheiten zur API finden Sie CreateTemplatein der AWS SDK für .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Create an Amazon Simple Email Service (Amazon SES) template.
/*!
```

```
  \param templateName: The name of the template.
  \param htmlPart: The HTML body of the email.
  \param subjectPart: The subject line of the email.
  \param textPart: The plain text version of the email.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::createTemplate(const Aws::String &templateName,
                                 const Aws::String &htmlPart,
                                 const Aws::String &subjectPart,
                                 const Aws::String &textPart,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::CreateTemplateRequest createTemplateRequest;
    Aws::SES::Model::Template aTemplate;

    aTemplate.SetTemplateName(templateName);
    aTemplate.SetHtmlPart(htmlPart);
    aTemplate.SetSubjectPart(subjectPart);
    aTemplate.SetTextPart(textPart);

    createTemplateRequest.SetTemplate(aTemplate);

    Aws::SES::Model::CreateTemplateOutcome outcome = sesClient.CreateTemplate(
            createTemplateRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully created template." << templateName << "."
                  << std::endl;
    }
    else {
        std::cerr << "Error creating template. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateTemplatein der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { CreateTemplateCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const TEMPLATE_NAME = getUniqueName("TestTemplateName");

const createCreateTemplateCommand = () => {
  return new CreateTemplateCommand({
    /**
     * The template feature in Amazon SES is based on the Handlebars template
 system.
     */
    Template: {
      /**
       * The name of an existing template in Amazon SES.
       */
      TemplateName: TEMPLATE_NAME,
      HtmlPart: `
        <h1>Hello, {{contact.firstName}}!</h1>
        <p>
        Did you know Amazon has a mascot named Peccy?
        </p>
      `,
      SubjectPart: "Amazon Tip",
    },
  });
};

const run = async () => {
  const createTemplateCommand = createCreateTemplateCommand();
```

```
  try {
    return await sesClient.send(createTemplateCommand);
  } catch (err) {
    console.log("Failed to create template.", err);
    return err;
  }
};
```

- Einzelheiten zur API finden Sie CreateTemplatein der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
```

```
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def create_template(self, name, subject, text, html):
        """
        Creates an email template.

        :param name: The name of the template.
        :param subject: The subject of the email.
        :param text: The plain text version of the email.
        :param html: The HTML version of the email.
        """
        try:
            template = {
                "TemplateName": name,
                "SubjectPart": subject,
                "TextPart": text,
                "HtmlPart": html,
            }
            self.ses_client.create_template(Template=template)
            logger.info("Created template %s.", name)
            self.template = template
            self._extract_tags(subject, text, html)
        except ClientError:
            logger.exception("Couldn't create template %s.", name)
            raise
```

- Einzelheiten zur API finden Sie CreateTemplatein AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
DATA(lo_template) = NEW /aws1/cl_sestemplate(
  iv_templatename = iv_name
  iv_subjectpart = iv_subject
  iv_textpart = iv_text
  iv_htmlpart = iv_html
).

TRY.
    lo_ses->createtemplate( io_template = lo_template ).
    MESSAGE 'Template created successfully' TYPE 'I'.
  CATCH /aws1/cx_sesalreadyexistsex INTO DATA(lo_ex1).
    DATA(lv_error) = |Template already exists: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
  CATCH /aws1/cx_sesinvalidtemplateex INTO DATA(lo_ex2).
    lv_error = |Invalid template: { lo_ex2->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex2.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex_generic.
ENDTRY.
```

- Einzelheiten zur API finden Sie CreateTemplatein der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DeleteIdentity`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DeleteIdentity` verwendet wird.

Aktionsbeispiele sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Sie können diese Aktion in den folgenden Codebeispielen im Kontext sehen:

- Amazon Simple Email Service (SES) einrichten
- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/// <summary>
/// Delete an email identity.
/// </summary>
/// <param name="identityEmail">The identity email to delete.</param>
/// <returns>True if successful.</returns>
public async Task<bool> DeleteIdentityAsync(string identityEmail)
{
    var success = false;
    try
    {
        var response = await _amazonSimpleEmailService.DeleteIdentityAsync(
            new DeleteIdentityRequest
            {
                Identity = identityEmail
            });
        success = response.HttpStatusCode == HttpStatusCode.OK;
    }
    catch (Exception ex)
    {
```

```
            Console.WriteLine("DeleteIdentityAsync failed with exception: " +
 ex.Message);
        }

        return success;
    }
```

- Einzelheiten zur API finden Sie DeleteIdentityin der AWS SDK für .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Delete the specified identity (an email address or a domain).
/*!
  \param identity: The identity to delete.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteIdentity(const Aws::String &identity,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteIdentityRequest deleteIdentityRequest;

    deleteIdentityRequest.SetIdentity(identity);

    Aws::SES::Model::DeleteIdentityOutcome outcome = sesClient.DeleteIdentity(
            deleteIdentityRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted identity." << std::endl;
    }
```

```
    else {
        std::cerr << "Error deleting identity. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DeleteIdentityin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

So löschen Sie eine Identität

Im folgenden Beispiel wird mit dem `delete-identity`-Befehl eine Identität aus der Liste der mit Amazon SES verifizierten Identitäten gelöscht:

```
aws ses delete-identity --identity user@example.com
```

Weitere Informationen zu verifizierten Identitäten finden Sie unter „Verifizieren von E-Mail-Adressen und Domains in Amazon SES“ im Entwicklerhandbuch zu Amazon Simple Email Service.

- Einzelheiten zur API finden Sie DeleteIdentityin der AWS CLI Befehlsreferenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { DeleteIdentityCommand } from "@aws-sdk/client-ses";
```

```
import { sesClient } from "./libs/sesClient.js";

const IDENTITY_EMAIL = "fake@example.com";

const createDeleteIdentityCommand = (identityName) => {
  return new DeleteIdentityCommand({
    Identity: identityName,
  });
};

const run = async () => {
  const deleteIdentityCommand = createDeleteIdentityCommand(IDENTITY_EMAIL);

  try {
    return await sesClient.send(deleteIdentityCommand);
  } catch (err) {
    console.log("Failed to delete identity.", err);
    return err;
  }
};
```

- Einzelheiten zur API finden Sie DeleteIdentityin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
```

```
def delete_identity(self, identity):
    """
    Deletes an identity.

    :param identity: The identity to remove.
    """
    try:
        self.ses_client.delete_identity(Identity=identity)
        logger.info("Deleted identity %s.", identity)
    except ClientError:
        logger.exception("Couldn't delete identity %s.", identity)
        raise
```

- Einzelheiten zur API finden Sie DeleteIdentityin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_ses->deleteidentity( iv_identity = iv_identity ).
    MESSAGE 'Identity deleted successfully' TYPE 'I'.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.
ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteIdentityin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`DeleteReceiptFilter`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `DeleteReceiptFilter` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Delete an Amazon Simple Email Service (Amazon SES) receipt filter.
/*!
  \param receiptFilterName: The name for the receipt filter.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteReceiptFilter(const Aws::String &receiptFilterName,
                                      const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteReceiptFilterRequest deleteReceiptFilterRequest;

    deleteReceiptFilterRequest.SetFilterName(receiptFilterName);

    Aws::SES::Model::DeleteReceiptFilterOutcome outcome =
 sesClient.DeleteReceiptFilter(
            deleteReceiptFilterRequest);

    if (outcome.IsSuccess()) {
```

```
        std::cout << "Successfully deleted receipt filter." << std::endl;
    }
    else {
        std::cerr << "Error deleting receipt filter. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DeleteReceiptFilterin der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { DeleteReceiptFilterCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const RECEIPT_FILTER_NAME = getUniqueName("ReceiptFilterName");

const createDeleteReceiptFilterCommand = (filterName) => {
  return new DeleteReceiptFilterCommand({ FilterName: filterName });
};

const run = async () => {
  const deleteReceiptFilterCommand =
    createDeleteReceiptFilterCommand(RECEIPT_FILTER_NAME);

  try {
    return await sesClient.send(deleteReceiptFilterCommand);
  } catch (err) {
    console.log("Error deleting receipt filter.", err);
```

```
    return err;
  }
};
```

- Einzelheiten zur API finden Sie DeleteReceiptFilterin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def delete_receipt_filter(self, filter_name):
        """
        Deletes a receipt filter.

        :param filter_name: The name of the filter to delete.
        """
        try:
            self.ses_client.delete_receipt_filter(FilterName=filter_name)
            logger.info("Deleted receipt filter %s.", filter_name)
        except ClientError:
            logger.exception("Couldn't delete receipt filter %s.", filter_name)
```

```
            raise
```

- Einzelheiten zur API finden Sie DeleteReceiptFilterin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_ses->deletereceiptfilter( iv_filtername = iv_filter_name ).
    MESSAGE 'Receipt filter deleted successfully' TYPE 'I'.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.
ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteReceiptFilterin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`DeleteReceiptRule`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `DeleteReceiptRule` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Delete an Amazon Simple Email Service (Amazon SES) receipt rule.
/*!
  \param receiptRuleName: The name for the receipt rule.
  \param receiptRuleSetName: The name for the receipt rule set.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteReceiptRule(const Aws::String &receiptRuleName,
                                    const Aws::String &receiptRuleSetName,
                                    const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteReceiptRuleRequest deleteReceiptRuleRequest;

    deleteReceiptRuleRequest.SetRuleName(receiptRuleName);
    deleteReceiptRuleRequest.SetRuleSetName(receiptRuleSetName);

    Aws::SES::Model::DeleteReceiptRuleOutcome outcome =
 sesClient.DeleteReceiptRule(
            deleteReceiptRuleRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted receipt rule." << std::endl;
    }
    else {
        std::cout << "Error deleting receipt rule. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
```

```
}
```

- Einzelheiten zur API finden Sie DeleteReceiptRulein der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { DeleteReceiptRuleCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const RULE_NAME = getUniqueName("RuleName");
const RULE_SET_NAME = getUniqueName("RuleSetName");

const createDeleteReceiptRuleCommand = () => {
  return new DeleteReceiptRuleCommand({
    RuleName: RULE_NAME,
    RuleSetName: RULE_SET_NAME,
  });
};

const run = async () => {
  const deleteReceiptRuleCommand = createDeleteReceiptRuleCommand();
  try {
    return await sesClient.send(deleteReceiptRuleCommand);
  } catch (err) {
    console.log("Failed to delete receipt rule.", err);
    return err;
  }
};
```

- Einzelheiten zur API finden Sie DeleteReceiptRulein der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def delete_receipt_rule(self, rule_set_name, rule_name):
        """
        Deletes a rule.

        :param rule_set_name: The rule set that contains the rule to delete.
        :param rule_name: The rule to delete.
        """
        try:
            self.ses_client.delete_receipt_rule(
                RuleSetName=rule_set_name, RuleName=rule_name
            )
            logger.info("Removed rule %s from rule set %s.", rule_name,
 rule_set_name)
        except ClientError:
            logger.exception(
```

```
                "Couldn't remove rule %s from rule set %s.", rule_name,
rule_set_name
            )
            raise
```

- Einzelheiten zur API finden Sie DeleteReceiptRulein AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_ses->deletereceiptrule(
      iv_rulesetname = iv_rule_set_name
      iv_rulename = iv_rule_name
    ).
    MESSAGE 'Receipt rule deleted successfully' TYPE 'I'.
  CATCH /aws1/cx_sesrulesetdoesnotexex INTO DATA(lo_ex1).
    DATA(lv_error) = |Rule set does not exist: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex_generic.
ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteReceiptRulein der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`DeleteReceiptRuleSet`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `DeleteReceiptRuleSet` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Delete an Amazon Simple Email Service (Amazon SES) receipt rule set.
/*!
  \param receiptRuleSetName: The name for the receipt rule set.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteReceiptRuleSet(const Aws::String &receiptRuleSetName,
                                       const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteReceiptRuleSetRequest deleteReceiptRuleSetRequest;

    deleteReceiptRuleSetRequest.SetRuleSetName(receiptRuleSetName);

    Aws::SES::Model::DeleteReceiptRuleSetOutcome outcome =
 sesClient.DeleteReceiptRuleSet(
            deleteReceiptRuleSetRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted receipt rule set." << std::endl;
    }

    else {
```

```
        std::cerr << "Error deleting receipt rule set. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DeleteReceiptRuleSetin der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { DeleteReceiptRuleSetCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const RULE_SET_NAME = getUniqueName("RuleSetName");

const createDeleteReceiptRuleSetCommand = () => {
  return new DeleteReceiptRuleSetCommand({ RuleSetName: RULE_SET_NAME });
};

const run = async () => {
  const deleteReceiptRuleSetCommand = createDeleteReceiptRuleSetCommand();

  try {
    return await sesClient.send(deleteReceiptRuleSetCommand);
  } catch (err) {
    console.log("Failed to delete receipt rule set.", err);
    return err;
  }
```

```
};
```

- Einzelheiten zur API finden Sie DeleteReceiptRuleSetin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def delete_receipt_rule_set(self, rule_set_name):
        """
        Deletes a rule set. When a rule set is deleted, all of the rules it
 contains
        are also deleted.

        :param rule_set_name: The name of the rule set to delete.
        """
        try:
            self.ses_client.delete_receipt_rule_set(RuleSetName=rule_set_name)
            logger.info("Deleted rule set %s.", rule_set_name)
        except ClientError:
            logger.exception("Couldn't delete rule set %s.", rule_set_name)
```

```
            raise
```

- Einzelheiten zur API finden Sie DeleteReceiptRuleSetin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_ses->deletereceiptruleset( iv_rulesetname = iv_rule_set_name ).
    MESSAGE 'Receipt rule set deleted successfully' TYPE 'I'.
  CATCH /aws1/cx_sescannotdeleteex INTO DATA(lo_ex1).
    DATA(lv_error) = |Cannot delete rule set: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex_generic.
ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteReceiptRuleSetin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`DeleteTemplate`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `DeleteTemplate` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Delete an email template.
    /// </summary>
    /// <param name="templateName">Name of the template.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailTemplateAsync(string templateName)
    {
        var success = false;
        try
        {
            var response = await _amazonSimpleEmailService.DeleteTemplateAsync(
                new DeleteTemplateRequest
                {
                    TemplateName = templateName
                });
            success = response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Exception ex)
        {
            Console.WriteLine("DeleteEmailTemplateAsync failed with exception: "
+ ex.Message);
        }
```

```
        return success;
    }
```

- Einzelheiten zur API finden Sie DeleteTemplatein der AWS SDK für .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Delete an Amazon Simple Email Service (Amazon SES) template.
/*!
  \param templateName: The name for the template.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteTemplate(const Aws::String &templateName,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteTemplateRequest deleteTemplateRequest;

    deleteTemplateRequest.SetTemplateName(templateName);

    Aws::SES::Model::DeleteTemplateOutcome outcome = sesClient.DeleteTemplate(
            deleteTemplateRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted template." << std::endl;
    }
    else {
        std::cerr << "Error deleting template. " <<
 outcome.GetError().GetMessage()
```

```
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DeleteTemplatein der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { DeleteTemplateCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const TEMPLATE_NAME = getUniqueName("TemplateName");

const createDeleteTemplateCommand = (templateName) =>
  new DeleteTemplateCommand({ TemplateName: templateName });

const run = async () => {
  const deleteTemplateCommand = createDeleteTemplateCommand(TEMPLATE_NAME);

  try {
    return await sesClient.send(deleteTemplateCommand);
  } catch (err) {
    console.log("Failed to delete template.", err);
    return err;
  }
};
```

- Einzelheiten zur API finden Sie DeleteTemplatein der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
 html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def delete_template(self):
        """
        Deletes an email template.
        """
```

```
        try:

self.ses_client.delete_template(TemplateName=self.template["TemplateName"])
            logger.info("Deleted template %s.", self.template["TemplateName"])
            self.template = None
            self.template_tags = None
        except ClientError:
            logger.exception(
                "Couldn't delete template %s.", self.template["TemplateName"]
            )
            raise
```

- Einzelheiten zur API finden Sie DeleteTemplatein AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    TRY.
        lo_ses->deletetemplate( iv_templatename = iv_template_name ).
        MESSAGE 'Template deleted successfully' TYPE 'I'.
      CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
        DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex.
    ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteTemplatein der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`DescribeReceiptRuleSet`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `DescribeReceiptRuleSet` verwendet wird.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def describe_receipt_rule_set(self, rule_set_name):
        """
        Gets data about a rule set.

        :param rule_set_name: The name of the rule set to retrieve.
        :return: Data about the rule set.
        """
        try:
            response = self.ses_client.describe_receipt_rule_set(
                RuleSetName=rule_set_name
            )
            logger.info("Got data for rule set %s.", rule_set_name)
```

```
        except ClientError:
            logger.exception("Couldn't get data for rule set %s.", rule_set_name)
            raise
        else:
            return response
```

- Einzelheiten zur API finden Sie DescribeReceiptRuleSetin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    oo_result = lo_ses->describereceiptruleset(
      iv_rulesetname = iv_rule_set_name
    ).
    MESSAGE 'Receipt rule set described successfully' TYPE 'I'.
  CATCH /aws1/cx_sesrulesetdoesnotexex INTO DATA(lo_ex1).
    DATA(lv_error) = |Rule set does not exist: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex_generic.
ENDTRY.
```

- Einzelheiten zur API finden Sie DescribeReceiptRuleSetin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetIdentityVerificationAttributes`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `GetIdentityVerificationAttributes` verwendet wird.

Aktionsbeispiele sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Sie können diese Aktion in den folgenden Codebeispielen im Kontext sehen:

- Amazon Simple Email Service (SES) einrichten
- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Get identity verification status for an email.
    /// </summary>
    /// <returns>The verification status of the email.</returns>
    public async Task<VerificationStatus> GetIdentityStatusAsync(string email)
    {
        var result = VerificationStatus.TemporaryFailure;
        try
        {
            var response =
                await
_amazonSimpleEmailService.GetIdentityVerificationAttributesAsync(
                    new GetIdentityVerificationAttributesRequest
                    {
```

```
                        Identities = new List<string> { email }
                    });

            if (response.VerificationAttributes.ContainsKey(email))
                result =
response.VerificationAttributes[email].VerificationStatus;
        }
        catch (Exception ex)
        {
            Console.WriteLine("GetIdentityStatusAsync failed with exception: " +
ex.Message);
        }

        return result;
    }
```

- Einzelheiten zur API finden Sie GetIdentityVerificationAttributesin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So rufen Sie den Bestätigungsstatus von Amazon SES für eine Liste der Identitäten ab

Im folgenden Beispiel wird der `get-identity-verification-attributes`-Befehl verwendet, um den Amazon-SES-Bestätigungsstatus für eine Liste der Identitäten abzurufen:

```
aws ses get-identity-verification-attributes --
identities "user1@example.com" "user2@example.com"
```

Ausgabe:

```
{
    "VerificationAttributes": {
        "user1@example.com": {
            "VerificationStatus": "Success"
        },
        "user2@example.com": {
            "VerificationStatus": "Pending"
```

```
        }
    }
}
```

Wenn Sie diesen Befehl mit einer Identität aufrufen, die Sie noch nie zur Überprüfung eingereicht haben, wird diese Identität nicht in der Ausgabe angezeigt.

Weitere Informationen zu verifizierten Identitäten finden Sie unter „Verifizieren von E-Mail-Adressen und Domains in Amazon SES“ im Entwicklerhandbuch zu Amazon Simple Email Service.

- Einzelheiten zur API finden Sie GetIdentityVerificationAttributesin der AWS CLI Befehlsreferenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def get_identity_status(self, identity):
        """
        Gets the status of an identity. This can be used to discover whether
        an identity has been successfully verified.

        :param identity: The identity to query.
        :return: The status of the identity.
```

```
        """
        try:
            response = self.ses_client.get_identity_verification_attributes(
                Identities=[identity]
            )
            status = response["VerificationAttributes"].get(
                identity, {"VerificationStatus": "NotFound"}
            )["VerificationStatus"]
            logger.info("Got status of %s for %s.", status, identity)
        except ClientError:
            logger.exception("Couldn't get status for %s.", identity)
            raise
        else:
            return status
```

- Einzelheiten zur API finden Sie GetIdentityVerificationAttributesin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
require 'aws-sdk-ses' # v2: require 'aws-sdk'

# Create client in us-west-2 region
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
client = Aws::SES::Client.new(region: 'us-west-2')

# Get up to 1000 identities
ids = client.list_identities({
                               identity_type: 'EmailAddress'
                             })
```

```
ids.identities.each do |email|
  attrs = client.get_identity_verification_attributes({
                                                        identities: [email]
                                                      })

  status = attrs.verification_attributes[email].verification_status

  # Display email addresses that have been verified
  puts email if status == 'Success'
end
```

- Einzelheiten zur API finden Sie GetIdentityVerificationAttributesin der AWS SDK für Ruby API-Referenz.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    DATA lt_identities TYPE /aws1/cl_sesidentitylist_w=>tt_identitylist.
    APPEND NEW /aws1/cl_sesidentitylist_w( iv_value = iv_identity ) TO
 lt_identities.

    TRY.
        DATA(lo_result) = lo_ses->getidentityverificationattrs(
          it_identities = lt_identities
        ).

        DATA(lt_attrs) = lo_result->get_verificationattributes( ).
        IF lt_attrs IS NOT INITIAL.
          LOOP AT lt_attrs ASSIGNING FIELD-SYMBOL(<ls_attr>).
            ov_status = <ls_attr>-value->get_verificationstatus( ).
            EXIT.
          ENDLOOP.
```

```
      ELSE.
        ov_status = 'NotFound'.
      ENDIF.
    CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
      DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
      MESSAGE lv_error TYPE 'I'.
      RAISE EXCEPTION lo_ex.
  ENDTRY.
```

- Einzelheiten zur API finden Sie GetIdentityVerificationAttributesin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetSendQuota`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `GetSendQuota` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Amazon Simple Email Service (SES) einrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/// <summary>
/// Get information on the current account's send quota.
/// </summary>
```

```
    /// <returns>The send quota response data.</returns>
    public async Task<GetSendQuotaResponse> GetSendQuotaAsync()
    {
        var result = new GetSendQuotaResponse();
        try
        {
            var response = await _amazonSimpleEmailService.GetSendQuotaAsync(
                new GetSendQuotaRequest());
            result = response;
        }
        catch (Exception ex)
        {
            Console.WriteLine("GetSendQuotaAsync failed with exception: " +
 ex.Message);
        }

        return result;
    }
```

- Einzelheiten zur API finden Sie GetSendQuotain der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So verwalten Sie Ihre Amazon-SES-Sendelimits

Im folgenden Beispiel wird der `get-send-quota`-Befehl verwendet, um Ihre Amazon-SES-Sendelimits zurückzugeben:

```
aws ses get-send-quota
```

Ausgabe:

```
{
   "Max24HourSend": 200.0,
   "SentLast24Hours": 1.0,
   "MaxSendRate": 1.0
}
```

Max24 HourSend ist Ihr Sendekontingent, das ist die maximale Anzahl von E-Mails, die Sie in einem Zeitraum von 24 Stunden versenden können. Die Sendequote bezieht sich auf einen gleitenden Zeitraum. Wenn Sie versuchen eine, E-Mail zu senden, überprüft Amazon SES, wie viele E-Mails Sie in den letzten 24 Stunden gesendet haben. Solange die Gesamtzahl der von Ihnen gesendeten E-Mails unter Ihrer Quote liegt, wird Ihre Sendeanforderung akzeptiert und Ihre E-Mail versendet.

SentLast24 Stunden ist die Anzahl der E-Mails, die Sie in den letzten 24 Stunden gesendet haben.

MaxSendRate ist die maximale Anzahl von E-Mails, die Sie pro Sekunde versenden können.

Beachten Sie, dass Sendelimits auf der Anzahl der Empfänger, nicht der Anzahl der Nachrichten basieren. Beispielsweise zählt eine E-Mail mit 10 Empfängern bei Ihrem Sendekontingent als 10.

Weitere Informationen finden Sie unter „Verwalten Ihrer Amazon-SES-Sendelimits“ im Entwicklerhandbuch zu Amazon Simple Email Service.

- Einzelheiten zur API finden Sie GetSendQuotain der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieser Befehl gibt die aktuellen Sende-Limits des Benutzers zurück.

```
Get-SESSendQuota
```

- Einzelheiten zur API finden Sie unter GetSendQuota AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: Dieser Befehl gibt die aktuellen Sende-Limits des Benutzers zurück.

```
Get-SESSendQuota
```

- Einzelheiten zur API finden Sie unter GetSendQuota AWS -Tools für PowerShellCmdlet-Referenz (V5).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Amazon SES mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`GetSendStatistics`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `GetSendStatistics` verwendet wird.

CLI

AWS CLI

So rufen Sie Ihre Amazon-SES-Sendestatistiken ab

Im folgenden Beispiel wird der `get-send-statistics`-Befehl verwendet, um Ihre Amazon-SES-Sendestatistiken zurückzugeben

```
aws ses get-send-statistics
```

Ausgabe:

```
{
   "SendDataPoints": [
       {
           "Complaints": 0,
           "Timestamp": "2013-06-12T19:32:00Z",
           "DeliveryAttempts": 2,
           "Bounces": 0,
           "Rejects": 0
       },
       {
           "Complaints": 0,
           "Timestamp": "2013-06-12T00:47:00Z",
           "DeliveryAttempts": 1,
           "Bounces": 0,
           "Rejects": 0
       }
   ]
}
```

Das Ergebnis ist eine Liste mit Datenpunkten, die die letzten zwei Wochen Sendeaktivität repräsentieren. Jeder Datenpunkt in der Liste enthält Statistiken für ein Intervall von 15 Minuten.

In diesem Beispiel gibt es nur zwei Datenpunkte, da die einzigen E-Mails, die der Benutzer in den letzten zwei Wochen gesendet hat, in zwei 15-Minuten-Intervalle fielen.

Weitere Informationen finden Sie unter „Verwalten Ihrer Amazon SES-Nutzungsstatistiken“ im Entwicklerhandbuch für Amazon Simple Email Service.

- Einzelheiten zur API finden Sie GetSendStatisticsin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieser Befehl gibt die Sendestatistik des Benutzers zurück. Das Ergebnis ist eine Liste mit Datenpunkten, die die letzten zwei Wochen Sendeaktivität repräsentieren. Jeder Datenpunkt in der Liste enthält Statistiken für ein Intervall von 15 Minuten.

```
Get-SESSendStatistic
```

- Einzelheiten zur API finden Sie unter GetSendStatistics AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: Dieser Befehl gibt die Sendestatistik des Benutzers zurück. Das Ergebnis ist eine Liste mit Datenpunkten, die die letzten zwei Wochen Sendeaktivität repräsentieren. Jeder Datenpunkt in der Liste enthält Statistiken für ein Intervall von 15 Minuten.

```
Get-SESSendStatistic
```

- Einzelheiten zur API finden Sie unter GetSendStatistics AWS -Tools für PowerShellCmdlet-Referenz (V5).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Amazon SES mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

GetTemplateMit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `GetTemplate` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Get a template's attributes.
/*!
  \param templateName: The name for the template.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::getTemplate(const Aws::String &templateName,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::GetTemplateRequest getTemplateRequest;

    getTemplateRequest.SetTemplateName(templateName);

    Aws::SES::Model::GetTemplateOutcome outcome = sesClient.GetTemplate(
            getTemplateRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully got template." << std::endl;
    }

    else {
```

```
        std::cerr << "Error getting template. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie GetTemplatein der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { GetTemplateCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const TEMPLATE_NAME = getUniqueName("TemplateName");

const createGetTemplateCommand = (templateName) =>
  new GetTemplateCommand({ TemplateName: templateName });

const run = async () => {
  const getTemplateCommand = createGetTemplateCommand(TEMPLATE_NAME);

  try {
    return await sesClient.send(getTemplateCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
```

```
    throw caught;
  }
};
```

- Einzelheiten zur API finden Sie GetTemplatein der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
 html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def get_template(self, name):
```

```
        """
        Gets a previously created email template.

        :param name: The name of the template to retrieve.
        :return: The retrieved email template.
        """
        try:
            response = self.ses_client.get_template(TemplateName=name)
            self.template = response["Template"]
            logger.info("Got template %s.", name)
            self._extract_tags(
                self.template["SubjectPart"],
                self.template["TextPart"],
                self.template["HtmlPart"],
            )
        except ClientError:
            logger.exception("Couldn't get template %s.", name)
            raise
        else:
            return self.template
```

- Einzelheiten zur API finden Sie GetTemplatein AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   TRY.
       DATA(lo_result) = lo_ses->gettemplate( iv_templatename =
iv_template_name ).
       oo_template = lo_result->get_template( ).
       MESSAGE 'Template retrieved successfully' TYPE 'I'.
     CATCH /aws1/cx_sestmpldoesnotexistex INTO DATA(lo_ex1).
       DATA(lv_error) = |Template does not exist: { lo_ex1->get_text( ) }|.
```

```
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex1.
      CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
        lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex_generic.
    ENDTRY.
```

- Einzelheiten zur API finden Sie GetTemplatein der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ListIdentities`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `ListIdentities` verwendet wird.

Aktionsbeispiele sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Sie können diese Aktion in den folgenden Codebeispielen im Kontext sehen:

- Kopieren von E-Mail- und Domain-Identitäten von Region zu Region
- Amazon Simple Email Service (SES) einrichten
- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/// <summary>
/// Get the identities of a specified type for the current account.
```

```
    /// </summary>
    /// <param name="identityType">IdentityType to list.</param>
    /// <returns>The list of identities.</returns>
    public async Task<List<string>> ListIdentitiesAsync(IdentityType
identityType)
    {
        var result = new List<string>();
        try
        {
            var response = await _amazonSimpleEmailService.ListIdentitiesAsync(
                new ListIdentitiesRequest
                {
                    IdentityType = identityType
                });
            result = response.Identities;
        }
        catch (Exception ex)
        {
            Console.WriteLine("ListIdentitiesAsync failed with exception: " +
ex.Message);
        }

        return result;
    }
```

- Einzelheiten zur API finden Sie ListIdentitiesin der AWS SDK für .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! List the identities associated with this account.
/*!
  \param identityType: The identity type enum. "NOT_SET" is a valid option.
```

```
  \param identities; A vector to receive the retrieved identities.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::listIdentities(Aws::SES::Model::IdentityType identityType,
                                 Aws::Vector<Aws::String> &identities,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::ListIdentitiesRequest listIdentitiesRequest;

    if (identityType != Aws::SES::Model::IdentityType::NOT_SET) {
        listIdentitiesRequest.SetIdentityType(identityType);
    }

    Aws::String nextToken; // Used for paginated results.
    do {
        if (!nextToken.empty()) {
            listIdentitiesRequest.SetNextToken(nextToken);
        }
        Aws::SES::Model::ListIdentitiesOutcome outcome =
 sesClient.ListIdentities(
                listIdentitiesRequest);

        if (outcome.IsSuccess()) {
            const auto &retrievedIdentities =
 outcome.GetResult().GetIdentities();
            if (!retrievedIdentities.empty()) {
                identities.insert(identities.cend(),
 retrievedIdentities.cbegin(),
                                  retrievedIdentities.cend());
            }
            nextToken = outcome.GetResult().GetNextToken();
        }
        else {
            std::cout << "Error listing identities. " <<
 outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!nextToken.empty());

    return true;
```

```
}
```

- Einzelheiten zur API finden Sie ListIdentitiesin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Um alle Identitäten (E-Mail-Adressen und Domains) für ein bestimmtes AWS Konto aufzulisten

Im folgenden Beispiel wird der `list-identities`-Befehl verwendet, um alle Identitäten aufzulisten, die zur Überprüfung bei Amazon SES eingereicht wurden:

```
aws ses list-identities
```

Ausgabe:

```
{
    "Identities": [
      "user@example.com",
      "example.com"
    ]
}
```

Die zurückgegebene Liste enthält alle Identitäten unabhängig vom Überprüfungsstatus (verifiziert, Überprüfung ausstehend, fehlgeschlagen usw.).

In diesem Beispiel werden E-Mail-Adressen und Domains zurückgegeben, weil wir den Parameter identity-type nicht angegeben haben.

Weitere Informationen zu verifizierten Identitäten finden Sie unter „Verifizieren von E-Mail-Adressen und Domains in Amazon SES“ im Entwicklerhandbuch zu Amazon Simple Email Service.

- Einzelheiten zur API finden Sie ListIdentitiesin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import software.amazon.awssdk.services.ses.model.ListIdentitiesResponse;
import software.amazon.awssdk.services.ses.model.SesException;
import java.io.IOException;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class ListIdentities {

    public static void main(String[] args) throws IOException {
        Region region = Region.US_WEST_2;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        listSESIdentities(client);
    }

    public static void listSESIdentities(SesClient client) {
        try {
            ListIdentitiesResponse identitiesResponse = client.listIdentities();
            List<String> identities = identitiesResponse.identities();
            for (String identity : identities) {
```

```
                System.out.println("The identity is " + identity);
            }

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

- Einzelheiten zur API finden Sie ListIdentitiesin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { ListIdentitiesCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const createListIdentitiesCommand = () =>
  new ListIdentitiesCommand({ IdentityType: "EmailAddress", MaxItems: 10 });

const run = async () => {
  const listIdentitiesCommand = createListIdentitiesCommand();

  try {
    return await sesClient.send(listIdentitiesCommand);
  } catch (err) {
    console.log("Failed to list identities.", err);
    return err;
  }
};
```

- Einzelheiten zur API finden Sie ListIdentitiesin der AWS SDK für JavaScript API-Referenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieser Befehl gibt eine Liste zurück, die alle Identitäten (E-Mail-Adressen und Domains) für ein bestimmtes AWS Konto enthält, unabhängig vom Bestätigungsstatus.

```
Get-SESIdentity
```

- Einzelheiten zur API finden Sie unter ListIdentities AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: Dieser Befehl gibt eine Liste zurück, die alle Identitäten (E-Mail-Adressen und Domains) für ein bestimmtes AWS Konto enthält, unabhängig vom Bestätigungsstatus.

```
Get-SESIdentity
```

- Einzelheiten zur API finden Sie unter ListIdentities AWS -Tools für PowerShellCmdlet-Referenz (V5).

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
```

```
        """
        self.ses_client = ses_client


    def list_identities(self, identity_type, max_items):
        """
        Gets the identities of the specified type for the current account.

        :param identity_type: The type of identity to retrieve, such as
EmailAddress.
        :param max_items: The maximum number of identities to retrieve.
        :return: The list of retrieved identities.
        """
        try:
            response = self.ses_client.list_identities(
                IdentityType=identity_type, MaxItems=max_items
            )
            identities = response["Identities"]
            logger.info("Got %s identities for the current account.",
len(identities))
        except ClientError:
            logger.exception("Couldn't list identities for the current account.")
            raise
        else:
            return identities
```

- Einzelheiten zur API finden Sie ListIdentitiesin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
require 'aws-sdk-ses' # v2: require 'aws-sdk'

# Create client in us-west-2 region
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
client = Aws::SES::Client.new(region: 'us-west-2')

# Get up to 1000 identities
ids = client.list_identities({
                               identity_type: 'EmailAddress'
                             })

ids.identities.each do |email|
  attrs = client.get_identity_verification_attributes({
                                                        identities: [email]
                                                      })

  status = attrs.verification_attributes[email].verification_status

  # Display email addresses that have been verified
  puts email if status == 'Success'
end
```

- Einzelheiten zur API finden Sie ListIdentitiesin der AWS SDK für Ruby API-Referenz.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    TRY.
        DATA(lo_result) = lo_ses->listidentities(
          iv_identitytype = iv_identity_type
          iv_maxitems = iv_max_items
        ).
        ot_identities = lo_result->get_identities( ).
        MESSAGE 'Identities retrieved successfully' TYPE 'I'.
```

```
      CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
        DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex.
    ENDTRY.
```

- Einzelheiten zur API finden Sie ListIdentitiesin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`ListReceiptFilters`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `ListReceiptFilters` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! List the receipt filters associated with this account.
/*!
  \param filters; A vector of "ReceiptFilter" to receive the retrieved filters.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool
AwsDoc::SES::listReceiptFilters(Aws::Vector<Aws::SES::Model::ReceiptFilter>
 &filters,
                                const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);
    Aws::SES::Model::ListReceiptFiltersRequest listReceiptFiltersRequest;
```

```
    Aws::SES::Model::ListReceiptFiltersOutcome outcome =
 sesClient.ListReceiptFilters(
            listReceiptFiltersRequest);
    if (outcome.IsSuccess()) {
        auto &retrievedFilters = outcome.GetResult().GetFilters();
        if (!retrievedFilters.empty()) {
            filters.insert(filters.cend(), retrievedFilters.cbegin(),
                           retrievedFilters.cend());
        }
    }
    else {
        std::cerr << "Error retrieving IP address filters: "
                  << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie ListReceiptFiltersin der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { ListReceiptFiltersCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const createListReceiptFiltersCommand = () => new ListReceiptFiltersCommand({});

const run = async () => {
  const listReceiptFiltersCommand = createListReceiptFiltersCommand();

  return await sesClient.send(listReceiptFiltersCommand);
};
```

- Einzelheiten zur API finden Sie ListReceiptFiltersin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def list_receipt_filters(self):
        """
        Gets the list of receipt filters for the current account.

        :return: The list of receipt filters.
        """
        try:
            response = self.ses_client.list_receipt_filters()
            filters = response["Filters"]
            logger.info("Got %s receipt filters.", len(filters))
        except ClientError:
            logger.exception("Couldn't get receipt filters.")
            raise
        else:
```

```
            return filters
```

- Einzelheiten zur API finden Sie ListReceiptFiltersin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    DATA(lo_result) = lo_ses->listreceiptfilters( ).
    ot_filters = lo_result->get_filters( ).
    MESSAGE 'Receipt filters retrieved successfully' TYPE 'I'.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.
ENDTRY.
```

- Einzelheiten zur API finden Sie ListReceiptFiltersin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`ListTemplates`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `ListTemplates` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// List email templates for the current account.
    /// </summary>
    /// <returns>A list of template metadata.</returns>
    public async Task<List<TemplateMetadata>> ListEmailTemplatesAsync()
    {
        var result = new List<TemplateMetadata>();
        try
        {
            var response = await _amazonSimpleEmailService.ListTemplatesAsync(
                new ListTemplatesRequest());
            result = response.TemplatesMetadata;
        }
        catch (Exception ex)
        {
            Console.WriteLine("ListEmailTemplatesAsync failed with exception: " +
ex.Message);
        }

        return result;
    }
```

- Einzelheiten zur API finden Sie ListTemplatesin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sesv2.SesV2Client;
import software.amazon.awssdk.services.sesv2.model.ListEmailTemplatesRequest;
import software.amazon.awssdk.services.sesv2.model.ListEmailTemplatesResponse;
import software.amazon.awssdk.services.sesv2.model.SesV2Exception;

public class ListTemplates {

    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
        SesV2Client sesv2Client = SesV2Client.builder()
                .region(region)
                .build();

        listAllTemplates(sesv2Client);
    }

    public static void listAllTemplates(SesV2Client sesv2Client) {
        try {
            ListEmailTemplatesRequest templatesRequest =
 ListEmailTemplatesRequest.builder()
                    .pageSize(1)
                    .build();

            ListEmailTemplatesResponse response =
 sesv2Client.listEmailTemplates(templatesRequest);
            response.templatesMetadata()
                    .forEach(template -> System.out.println("Template name: " +
 template.templateName()));

        } catch (SesV2Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
```

```
            System.exit(1);
        }
    }
}
```

- Einzelheiten zur API finden Sie ListTemplatesin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { ListTemplatesCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const createListTemplatesCommand = (maxItems) =>
  new ListTemplatesCommand({ MaxItems: maxItems });

const run = async () => {
  const listTemplatesCommand = createListTemplatesCommand(10);

  try {
    return await sesClient.send(listTemplatesCommand);
  } catch (err) {
    console.log("Failed to list templates.", err);
    return err;
  }
};
```

- Einzelheiten zur API finden Sie ListTemplatesin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
 html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def list_templates(self):
        """
        Gets a list of all email templates for the current account.

        :return: The list of retrieved email templates.
        """
        try:
            response = self.ses_client.list_templates()
```

```
            templates = response["TemplatesMetadata"]
            logger.info("Got %s templates.", len(templates))
        except ClientError:
            logger.exception("Couldn't get templates.")
            raise
        else:
            return templates
```

- Einzelheiten zur API finden Sie ListTemplatesin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    DATA(lo_result) = lo_ses->listtemplates( iv_maxitems = iv_max_items ).
    ot_templates = lo_result->get_templatesmetadata( ).
    MESSAGE 'Templates retrieved successfully' TYPE 'I'.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.
ENDTRY.
```

- Einzelheiten zur API finden Sie ListTemplatesin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`SendBulkTemplatedEmail`Mit einem AWS SDK verwenden

Das folgende Codebeispiel zeigt, wie es verwendet wird`SendBulkTemplatedEmail`.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { SendBulkTemplatedEmailCommand } from "@aws-sdk/client-ses";
import {
  getUniqueName,
  postfix,
} from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

/**
 * Replace this with the name of an existing template.
 */
const TEMPLATE_NAME = getUniqueName("ReminderTemplate");

/**
 * Replace these with existing verified emails.
 */
const VERIFIED_EMAIL_1 = postfix(getUniqueName("Bilbo"), "@example.com");
const VERIFIED_EMAIL_2 = postfix(getUniqueName("Frodo"), "@example.com");

const USERS = [
  { firstName: "Bilbo", emailAddress: VERIFIED_EMAIL_1 },
  { firstName: "Frodo", emailAddress: VERIFIED_EMAIL_2 },
];

/**
 *
 * @param { { emailAddress: string, firstName: string }[] } users
 * @param { string } templateName the name of an existing template in SES
 * @returns { SendBulkTemplatedEmailCommand }
 */
```

```
const createBulkReminderEmailCommand = (users, templateName) => {
  return new SendBulkTemplatedEmailCommand({
    /**
     * Each 'Destination' uses a corresponding set of replacement data. We can
 map each user
     * to a 'Destination' and provide user specific replacement data to create
 personalized emails.
     *
     * Here's an example of how a template would be replaced with user data:
     * Template: <h1>Hello {{name}},</h1><p>Don't forget about the party gifts!</
p>
     * Destination 1: <h1>Hello Bilbo,</h1><p>Don't forget about the party gifts!
</p>
     * Destination 2: <h1>Hello Frodo,</h1><p>Don't forget about the party gifts!
</p>
     */
    Destinations: users.map((user) => ({
      Destination: { ToAddresses: [user.emailAddress] },
      ReplacementTemplateData: JSON.stringify({ name: user.firstName }),
    })),
    DefaultTemplateData: JSON.stringify({ name: "Shireling" }),
    Source: VERIFIED_EMAIL_1,
    Template: templateName,
  });
};

const run = async () => {
  const sendBulkTemplateEmailCommand = createBulkReminderEmailCommand(
    USERS,
    TEMPLATE_NAME,
  );
  try {
    return await sesClient.send(sendBulkTemplateEmailCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
  }
};
```

- Einzelheiten zur API finden Sie SendBulkTemplatedEmailin der AWS SDK für JavaScript API-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`SendEmail`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `SendEmail` verwendet wird.

Aktionsbeispiele sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Sie können diese Aktion in den folgenden Codebeispielen im Kontext sehen:

- Amazon Simple Email Service (SES) einrichten
- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/// <summary>
///  Send an email by using Amazon SES.
/// </summary>
/// <param name="toAddresses">List of recipients.</param>
/// <param name="ccAddresses">List of cc recipients.</param>
/// <param name="bccAddresses">List of bcc recipients.</param>
/// <param name="bodyHtml">Body of the email in HTML.</param>
/// <param name="bodyText">Body of the email in plain text.</param>
/// <param name="subject">Subject line of the email.</param>
/// <param name="senderAddress">From address.</param>
/// <returns>The messageId of the email.</returns>
public async Task<string> SendEmailAsync(List<string> toAddresses,
```

```
        List<string> ccAddresses, List<string> bccAddresses,
        string bodyHtml, string bodyText, string subject, string senderAddress)
    {
        var messageId = "";
        try
        {
            var response = await _amazonSimpleEmailService.SendEmailAsync(
                new SendEmailRequest
                {
                    Destination = new Destination
                    {
                        BccAddresses = bccAddresses,
                        CcAddresses = ccAddresses,
                        ToAddresses = toAddresses
                    },
                    Message = new Message
                    {
                        Body = new Body
                        {
                            Html = new Content
                            {
                                Charset = "UTF-8",
                                Data = bodyHtml
                            },
                            Text = new Content
                            {
                                Charset = "UTF-8",
                                Data = bodyText
                            }
                        },
                        Subject = new Content
                        {
                            Charset = "UTF-8",
                            Data = subject
                        }
                    },
                    Source = senderAddress
                });
            messageId = response.MessageId;
        }
        catch (Exception ex)
        {
            Console.WriteLine("SendEmailAsync failed with exception: " +
ex.Message);
```

```
        }

        return messageId;
    }
```

- Einzelheiten zur API finden Sie SendEmailin der AWS SDK für .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Send an email to a list of recipients.
/*!
  \param recipients; Vector of recipient email addresses.
  \param subject: Email subject.
  \param htmlBody: Email body as HTML. At least one body data is required.
  \param textBody: Email body as plain text. At least one body data is required.
  \param senderEmailAddress: Email address of sender. Ignored if empty string.
  \param ccAddresses: Vector of cc addresses. Ignored if empty.
  \param replyToAddress: Reply to email address. Ignored if empty string.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::sendEmail(const Aws::Vector<Aws::String> &recipients,
                            const Aws::String &subject,
                            const Aws::String &htmlBody,
                            const Aws::String &textBody,
                            const Aws::String &senderEmailAddress,
                            const Aws::Vector<Aws::String> &ccAddresses,
                            const Aws::String &replyToAddress,
                            const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);
```

```
    Aws::SES::Model::Destination destination;
    if (!ccAddresses.empty()) {
        destination.WithCcAddresses(ccAddresses);
    }
    if (!recipients.empty()) {
        destination.WithToAddresses(recipients);
    }

    Aws::SES::Model::Body message_body;
    if (!htmlBody.empty()) {
        message_body.SetHtml(

Aws::SES::Model::Content().WithCharset("UTF-8").WithData(htmlBody));
    }

    if (!textBody.empty()) {
        message_body.SetText(

Aws::SES::Model::Content().WithCharset("UTF-8").WithData(textBody));
    }

    Aws::SES::Model::Message message;
    message.SetBody(message_body);
    message.SetSubject(
            Aws::SES::Model::Content().WithCharset("UTF-8").WithData(subject));

    Aws::SES::Model::SendEmailRequest sendEmailRequest;
    sendEmailRequest.SetDestination(destination);
    sendEmailRequest.SetMessage(message);
    if (!senderEmailAddress.empty()) {
        sendEmailRequest.SetSource(senderEmailAddress);
    }
    if (!replyToAddress.empty()) {
        sendEmailRequest.AddReplyToAddresses(replyToAddress);
    }

    auto outcome = sesClient.SendEmail(sendEmailRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully sent message with ID "
                  << outcome.GetResult().GetMessageId()
                  << "." << std::endl;
    }
    else {
```

```
        std::cerr << "Error sending message. " << outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie SendEmailin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

So senden Sie eine formatierte E-Mail mit Amazon SES

Im folgenden Beispiel wird der `send-email`-Befehl verwendet, um eine formatierte E-Mail zu senden:

```
aws ses send-email --from sender@example.com --destination file://
destination.json --message file://message.json
```

Ausgabe:

```
{
   "MessageId": "EXAMPLEf3a5efcd1-51adec81-d2a4-4e3f-9fe2-5d85c1b23783-000000"
}
```

Das Ziel und die Nachricht sind JSON-Datenstrukturen, die in JSON-Dateien im aktuellen Verzeichnis gespeichert sind. Es handelt sich dabei um die folgenden Dateien:

`destination.json`:

```
{
  "ToAddresses":  ["recipient1@example.com", "recipient2@example.com"],
  "CcAddresses":  ["recipient3@example.com"],
  "BccAddresses": []
}
```

`message.json`:

```
{
   "Subject": {
       "Data": "Test email sent using the AWS CLI",
       "Charset": "UTF-8"
   },
   "Body": {
       "Text": {
           "Data": "This is the message body in text format.",
           "Charset": "UTF-8"
       },
       "Html": {
           "Data": "This message body contains HTML formatting. It can, for
 example, contain links like this one: <a class=\"ulink\" href=\"http://
docs.aws.amazon.com/ses/latest/DeveloperGuide\" target=\"_blank\">Amazon SES
 Developer Guide</a>.",
           "Charset": "UTF-8"
       }
   }
}
```

Ersetzen Sie die Absender- und Empfänger-E-Mail-Adressen durch die Adressen, die Sie verwenden möchten. Beachten Sie, dass die E-Mail-Adresse des Absenders mit Amazon SES verifiziert werden muss. Bis Ihnen Produktionszugriff auf Amazon SES gewährt wird, müssen Sie auch die E-Mail-Adresse jedes Empfängers verifizieren, es sei denn, es handelt sich bei dem Empfänger um den Amazon-SES-Postfachsimulator. Weitere Informationen zu verifizierten Identitäten finden Sie unter „Verifizieren von E-Mail-Adressen und Domains in Amazon SES“ im Entwicklerhandbuch zu Amazon Simple Email Service.

Die Nachrichten-ID in der Ausgabe gibt an, dass der Aufruf von send-email erfolgreich war.

Wenn Sie die E-Mail nicht erhalten, überprüfen Sie Ihr Junk-Postfach.

Weitere Informationen zum Senden formatierter E-Mails finden Sie unter „Senden formatierter E-Mails mit der Amazon-SES-API“ im Entwicklerhandbuch von Amazon Simple Email Service.

- Einzelheiten zur API finden Sie SendEmailin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import software.amazon.awssdk.services.ses.model.Content;
import software.amazon.awssdk.services.ses.model.Destination;
import software.amazon.awssdk.services.ses.model.Message;
import software.amazon.awssdk.services.ses.model.Body;
import software.amazon.awssdk.services.ses.model.SendEmailRequest;
import software.amazon.awssdk.services.ses.model.SesException;

import javax.mail.MessagingException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class SendMessageEmailRequest {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <sender> <recipient> <subject>\s

                Where:
                    sender - An email address that represents the sender.\s
                    recipient -  An email address that represents the recipient.
\s
                    subject - The  subject line.\s
```

```
                """;

        if (args.length != 3) {
            System.out.println(usage);
            System.exit(1);
        }

        String sender = args[0];
        String recipient = args[1];
        String subject = args[2];

        Region region = Region.US_EAST_1;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        // The HTML body of the email.
        String bodyHTML = "<html>" + "<head></head>" + "<body>" + "<h1>Hello!</
h1>"
                + "<p> See the list of customers.</p>" + "</body>" + "</html>";

        try {
            send(client, sender, recipient, subject, bodyHTML);
            client.close();
            System.out.println("Done");

        } catch (MessagingException e) {
            e.printStackTrace();
        }
    }

    public static void send(SesClient client,
            String sender,
            String recipient,
            String subject,
            String bodyHTML) throws MessagingException {

        Destination destination = Destination.builder()
                .toAddresses(recipient)
                .build();

        Content content = Content.builder()
                .data(bodyHTML)
                .build();
```

```
        Content sub = Content.builder()
                .data(subject)
                .build();

        Body body = Body.builder()
                .html(content)
                .build();

        Message msg = Message.builder()
                .subject(sub)
                .body(body)
                .build();

        SendEmailRequest emailRequest = SendEmailRequest.builder()
                .destination(destination)
                .message(msg)
                .source(sender)
                .build();

        try {
            System.out.println("Attempting to send an email through Amazon SES "
 + "using the AWS SDK for Java...");
            client.sendEmail(emailRequest);

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import javax.activation.DataHandler;
import javax.activation.DataSource;
import javax.mail.Message;
import javax.mail.MessagingException;
import javax.mail.Session;
import javax.mail.internet.AddressException;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;
import javax.mail.internet.MimeMultipart;
import javax.mail.internet.MimeBodyPart;
```

```
import javax.mail.util.ByteArrayDataSource;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.nio.ByteBuffer;
import java.nio.file.Files;
import java.util.Properties;
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.services.ses.model.SendRawEmailRequest;
import software.amazon.awssdk.services.ses.model.RawMessage;
import software.amazon.awssdk.services.ses.model.SesException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class SendMessageAttachment {
    public static void main(String[] args) throws IOException {
        final String usage = """

                Usage:
                    <sender> <recipient> <subject> <fileLocation>\s

                Where:
                    sender - An email address that represents the sender.\s
                    recipient -  An email address that represents the recipient.
\s
                    subject - The  subject line.\s
                    fileLocation - The location of a Microsoft Excel file to use
 as an attachment (C:/AWS/customers.xls).\s
                """;

        if (args.length != 4) {
            System.out.println(usage);
            System.exit(1);
        }

        String sender = args[0];
        String recipient = args[1];
```

```
        String subject = args[2];
        String fileLocation = args[3];

        // The email body for recipients with non-HTML email clients.
        String bodyText = "Hello,\r\n" + "Please see the attached file for a list
 "
                + "of customers to contact.";

        // The HTML body of the email.
        String bodyHTML = "<html>" + "<head></head>" + "<body>" + "<h1>Hello!</
h1>"
                + "<p>Please see the attached file for a " + "list of customers
 to contact.</p>" + "</body>"
                + "</html>";

        Region region = Region.US_WEST_2;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        try {
            sendemailAttachment(client, sender, recipient, subject, bodyText,
 bodyHTML, fileLocation);
            client.close();
            System.out.println("Done");

        } catch (IOException | MessagingException e) {
            e.printStackTrace();
        }
    }

    public static void sendemailAttachment(SesClient client,
            String sender,
            String recipient,
            String subject,
            String bodyText,
            String bodyHTML,
            String fileLocation) throws AddressException, MessagingException,
 IOException {

        java.io.File theFile = new java.io.File(fileLocation);
        byte[] fileContent = Files.readAllBytes(theFile.toPath());

        Session session = Session.getDefaultInstance(new Properties());
```

```
        // Create a new MimeMessage object.
        MimeMessage message = new MimeMessage(session);

        // Add subject, from and to lines.
        message.setSubject(subject, "UTF-8");
        message.setFrom(new InternetAddress(sender));
        message.setRecipients(Message.RecipientType.TO,
 InternetAddress.parse(recipient));

        // Create a multipart/alternative child container.
        MimeMultipart msgBody = new MimeMultipart("alternative");

        // Create a wrapper for the HTML and text parts.
        MimeBodyPart wrap = new MimeBodyPart();

        // Define the text part.
        MimeBodyPart textPart = new MimeBodyPart();
        textPart.setContent(bodyText, "text/plain; charset=UTF-8");

        // Define the HTML part.
        MimeBodyPart htmlPart = new MimeBodyPart();
        htmlPart.setContent(bodyHTML, "text/html; charset=UTF-8");

        // Add the text and HTML parts to the child container.
        msgBody.addBodyPart(textPart);
        msgBody.addBodyPart(htmlPart);

        // Add the child container to the wrapper object.
        wrap.setContent(msgBody);

        // Create a multipart/mixed parent container.
        MimeMultipart msg = new MimeMultipart("mixed");

        // Add the parent container to the message.
        message.setContent(msg);
        msg.addBodyPart(wrap);

        // Define the attachment.
        MimeBodyPart att = new MimeBodyPart();
        DataSource fds = new ByteArrayDataSource(fileContent,
                "application/vnd.openxmlformats-
officedocument.spreadsheetml.sheet");
        att.setDataHandler(new DataHandler(fds));
```

```
        String reportName = "WorkReport.xls";
        att.setFileName(reportName);

        // Add the attachment to the message.
        msg.addBodyPart(att);

        try {
            System.out.println("Attempting to send an email through Amazon SES "
 + "using the AWS SDK for Java...");

            ByteArrayOutputStream outputStream = new ByteArrayOutputStream();
            message.writeTo(outputStream);

            ByteBuffer buf = ByteBuffer.wrap(outputStream.toByteArray());

            byte[] arr = new byte[buf.remaining()];
            buf.get(arr);

            SdkBytes data = SdkBytes.fromByteArray(arr);
            RawMessage rawMessage = RawMessage.builder()
                    .data(data)
                    .build();

            SendRawEmailRequest rawEmailRequest = SendRawEmailRequest.builder()
                    .rawMessage(rawMessage)
                    .build();

            client.sendRawEmail(rawEmailRequest);

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        System.out.println("Email sent using SesClient with attachment");
    }
}
```

- Einzelheiten zur API finden Sie SendEmailin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { SendEmailCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const createSendEmailCommand = (toAddress, fromAddress) => {
  return new SendEmailCommand({
    Destination: {
      /* required */
      CcAddresses: [
        /* more items */
      ],
      ToAddresses: [
        toAddress,
        /* more To-email addresses */
      ],
    },
    Message: {
      /* required */
      Body: {
        /* required */
        Html: {
          Charset: "UTF-8",
          Data: "HTML_FORMAT_BODY",
        },
        Text: {
          Charset: "UTF-8",
          Data: "TEXT_FORMAT_BODY",
        },
      },
      Subject: {
        Charset: "UTF-8",
        Data: "EMAIL_SUBJECT",
      },
```

```
    },
    Source: fromAddress,
    ReplyToAddresses: [
      /* more items */
    ],
  });
};

const run = async () => {
  const sendEmailCommand = createSendEmailCommand(
    "recipient@example.com",
    "sender@example.com",
  );

  try {
    return await sesClient.send(sendEmailCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
  }
};
```

- Einzelheiten zur API finden Sie SendEmailin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesMailSender:
    """Encapsulates functions to send emails with Amazon SES."""
```

```
   def __init__(self, ses_client):
       """
       :param ses_client: A Boto3 Amazon SES client.
       """
       self.ses_client = ses_client


   def send_email(self, source, destination, subject, text, html,
reply_tos=None):
       """
       Sends an email.

       Note: If your account is in the Amazon SES  sandbox, the source and
       destination email accounts must both be verified.

       :param source: The source email account.
       :param destination: The destination email account.
       :param subject: The subject of the email.
       :param text: The plain text version of the body of the email.
       :param html: The HTML version of the body of the email.
       :param reply_tos: Email accounts that will receive a reply if the
recipient
                         replies to the message.
       :return: The ID of the message, assigned by Amazon SES.
       """
       send_args = {
           "Source": source,
           "Destination": destination.to_service_format(),
           "Message": {
               "Subject": {"Data": subject},
               "Body": {"Text": {"Data": text}, "Html": {"Data": html}},
           },
       }
       if reply_tos is not None:
           send_args["ReplyToAddresses"] = reply_tos
       try:
           response = self.ses_client.send_email(**send_args)
           message_id = response["MessageId"]
           logger.info(
               "Sent mail %s from %s to %s.", message_id, source,
destination.tos
           )
       except ClientError:
```

```
            logger.exception(
                "Couldn't send mail from %s to %s.", source, destination.tos
            )
            raise
        else:
            return message_id
```

- Einzelheiten zur API finden Sie SendEmailin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
require 'aws-sdk-ses' # v2: require 'aws-sdk'

# Replace sender@example.com with your "From" address.
# This address must be verified with Amazon SES.
sender = 'sender@example.com'

# Replace recipient@example.com with a "To" address. If your account
# is still in the sandbox, this address must be verified.
recipient = 'recipient@example.com'

# Specify a configuration set. To use a configuration
# set, uncomment the next line and line 74.
#   configsetname = "ConfigSet"

# The subject line for the email.
subject = 'Amazon SES test (AWS SDK for Ruby)'

# The HTML body of the email.
htmlbody =
  '<h1>Amazon SES test (AWS SDK for Ruby)</h1>'\
```

```
  '<p>This email was sent with <a href="https://aws.amazon.com/ses/">'\
  'Amazon SES</a> using the <a href="https://aws.amazon.com/sdk-for-ruby/">'\
  'AWS SDK for Ruby</a>.'

# The email body for recipients with non-HTML email clients.
textbody = 'This email was sent with Amazon SES using the AWS SDK for Ruby.'

# Specify the text encoding scheme.
encoding = 'UTF-8'

# Create a new SES client in the us-west-2 region.
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
ses = Aws::SES::Client.new(region: 'us-west-2')

# Try to send the email.
begin
  # Provide the contents of the email.
  ses.send_email(
    destination: {
      to_addresses: [
        recipient
      ]
    },
    message: {
      body: {
        html: {
          charset: encoding,
          data: htmlbody
        },
        text: {
          charset: encoding,
          data: textbody
        }
      },
      subject: {
        charset: encoding,
        data: subject
      }
    },
    source: sender
    # Uncomment the following line to use a configuration set.
    # configuration_set_name: configsetname,
  )
```

```
  puts "Email sent to #{recipient}"

# If something goes wrong, display an error message.
rescue Aws::SES::Errors::ServiceError => e
  puts "Email not sent. Error message: #{e}"
end
```

- Einzelheiten zur API finden Sie SendEmailin der AWS SDK für Ruby API-Referenz.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    " Create message object
    DATA(lo_subject) = NEW /aws1/cl_sescontent( iv_data = iv_subject ).
    DATA(lo_text_body) = NEW /aws1/cl_sescontent( iv_data = iv_text ).
    DATA(lo_html_body) = NEW /aws1/cl_sescontent( iv_data = iv_html ).
    DATA(lo_body) = NEW /aws1/cl_sesbody(
      io_text = lo_text_body
      io_html = lo_html_body
    ).
    DATA(lo_message) = NEW /aws1/cl_sesmessage(
      io_subject = lo_subject
      io_body = lo_body
    ).

    TRY.
        " Send email
        DATA(lo_result) = lo_ses->sendemail(
          iv_source = iv_source
          io_destination = io_destination
          io_message = lo_message
          it_replytoaddresses = it_reply_tos
        ).
        ov_msg_id = lo_result->get_messageid( ).
```

```
        MESSAGE 'Email sent successfully' TYPE 'I'.
      CATCH /aws1/cx_sesacctsendingpause00 INTO DATA(lo_ex1).
        DATA(lv_error) = |Account sending paused: { lo_ex1->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex1.
      CATCH /aws1/cx_sesmessagerejected INTO DATA(lo_ex2).
        lv_error = |Message rejected: { lo_ex2->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex2.
      CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
        lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex_generic.
    ENDTRY.
```

- Einzelheiten zur API finden Sie SendEmailin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`SendRawEmail`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `SendRawEmail` verwendet wird.

CLI

AWS CLI

So senden Sie eine RAW-E-Mail mit Amazon SES

Im folgenden Beispiel wird der `send-raw-email`-Befehl verwendet, um eine E-Mail mit einem TXT-Anhang zu senden:

```
aws ses send-raw-email --raw-message file://message.json
```

Ausgabe:

```
{
```

```
   "MessageId": "EXAMPLEf3f73d99b-c63fb06f-d263-41f8-a0fb-d0dc67d56c07-000000"
}
```

Die RAW-Nachricht ist eine JSON-Datenstruktur, die in einer Datei mit dem Namen `message.json` im aktuellen Verzeichnis gespeichert ist. Sie enthält Folgendes:

```
{
   "Data": "From: sender@example.com\nTo: recipient@example.com\nSubject:
 Test email sent using the AWS CLI (contains an attachment)\nMIME-Version:
 1.0\nContent-type: Multipart/Mixed; boundary=\"NextPart\"\n\n--NextPart
\nContent-Type: text/plain\n\nThis is the message body.\n\n--NextPart\nContent-
Type: text/plain;\nContent-Disposition: attachment; filename=\"attachment.txt\"\n
\nThis is the text in the attachment.\n\n--NextPart--"
}
```

Wie Sie sehen, ist „Data“ eine lange Zeichenfolge, die den gesamten RAW-E-Mail-Inhalt im MIME-Format enthält, einschließlich eines Anhangs namens attachment.txt.

Ersetzen Sie sender@example.com und recipient@example.com durch die Adressen, die Sie verwenden möchten. Beachten Sie, dass die E-Mail-Adresse des Absenders mit Amazon SES verifiziert werden muss. Bis Ihnen Produktionszugriff auf Amazon SES gewährt wird, müssen Sie auch die E-Mail-Adresse des Empfängers verifizieren, es sei denn, es handelt sich bei dem Empfänger um den Amazon-SES-Postfachsimulator. Weitere Informationen zu verifizierten Identitäten finden Sie unter „Verifizieren von E-Mail-Adressen und Domains in Amazon SES“ im Entwicklerhandbuch zu Amazon Simple Email Service.

Die Nachrichten-ID in der Ausgabe gibt an, dass der Aufruf von erfolgreich send-raw-email war.

Wenn Sie die E-Mail nicht erhalten, überprüfen Sie Ihr Junk-Postfach.

Weitere Informationen zum Senden von RAW-E-Mails finden Sie unter „Senden von RAW-E-Mails mit der Amazon-SES-API“ im Entwicklerhandbuch von Amazon Simple Email Service.

- Einzelheiten zur API finden Sie SendRawEmailin der AWS CLI Befehlsreferenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Verwenden Sie nodemailer, um eine E-Mail mit einem Anhang zu senden.

```
import sesClientModule from "@aws-sdk/client-ses";
/**
 * nodemailer wraps the SES SDK and calls SendRawEmail. Use this for more
 advanced
 * functionality like adding attachments to your email.
 *
 * https://nodemailer.com/transports/ses
 */
import nodemailer from "nodemailer";

/**
 * @param {string} from An Amazon SES verified email address.
 * @param {*} to An Amazon SES verified email address.
 */
export const sendEmailWithAttachments = (
  from = "from@example.com",
  to = "to@example.com",
) => {
  const ses = new sesClientModule.SESClient({});
  const transporter = nodemailer.createTransport({
    SES: { ses, aws: sesClientModule },
  });

  return new Promise((resolve, reject) => {
    transporter.sendMail(
      {
        from,
        to,
        subject: "Hello World",
        text: "Greetings from Amazon SES!",
        attachments: [{ content: "Hello World!", filename: "hello.txt" }],
```

```
      },
      (err, info) => {
        if (err) {
          reject(err);
        } else {
          resolve(info);
        }
      },
    );
  });
};
```

- Einzelheiten zur API finden Sie SendRawEmailin der AWS SDK für JavaScript API-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`SendTemplatedEmail`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `SendTemplatedEmail` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   /// <summary>
   /// Send an email using a template.
   /// </summary>
   /// <param name="sender">Address of the sender.</param>
   /// <param name="recipients">Addresses of the recipients.</param>
   /// <param name="templateName">Name of the email template.</param>
   /// <param name="templateDataObject">Data for the email template.</param>
   /// <returns>The messageId of the email.</returns>
   public async Task<string> SendTemplateEmailAsync(string sender, List<string>
recipients,
       string templateName, object templateDataObject)
   {
       var messageId = "";
       try
       {
           // Template data should be serialized JSON from either a class or a
dynamic object.
           var templateData = JsonSerializer.Serialize(templateDataObject);

           var response = await
_amazonSimpleEmailService.SendTemplatedEmailAsync(
               new SendTemplatedEmailRequest
               {
                   Source = sender,
                   Destination = new Destination
                   {
                       ToAddresses = recipients
                   },
                   Template = templateName,
                   TemplateData = templateData
               });
           messageId = response.MessageId;
       }
       catch (Exception ex)
       {
           Console.WriteLine("SendTemplateEmailAsync failed with exception: " +
ex.Message);
       }

       return messageId;
   }
```

- Einzelheiten zur API finden Sie SendTemplatedEmailin der AWS SDK für .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Send a templated email to a list of recipients.
/*!
  \param recipients; Vector of recipient email addresses.
  \param templateName: The name of the template to use.
  \param templateData: Map of key-value pairs for replacing text in template.
  \param senderEmailAddress: Email address of sender. Ignored if empty string.
  \param ccAddresses: Vector of cc addresses. Ignored if empty.
  \param replyToAddress: Reply to email address. Ignored if empty string.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::sendTemplatedEmail(const Aws::Vector<Aws::String> &recipients,
                                     const Aws::String &templateName,
                                     const Aws::Map<Aws::String, Aws::String>
 &templateData,
                                     const Aws::String &senderEmailAddress,
                                     const Aws::Vector<Aws::String> &ccAddresses,
                                     const Aws::String &replyToAddress,
                                     const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::Destination destination;
    if (!ccAddresses.empty()) {
        destination.WithCcAddresses(ccAddresses);
    }
    if (!recipients.empty()) {
        destination.WithToAddresses(recipients);
```

```
    }

    Aws::SES::Model::SendTtemplatedEmailRequest sendTemplatedEmailRequest;
    sendTemplatedEmailRequest.SetDestination(destination);
    sendTemplatedEmailRequest.SetTemplate(templateName);

    std::ostringstream templateDataStream;
    templateDataStream << "{";
    size_t dataCount = 0;
    for (auto &pair: templateData) {
        templateDataStream << "\"" << pair.first << "\":\"" << pair.second <<
 "\"";
        dataCount++;
        if (dataCount < templateData.size()) {
            templateDataStream << ",";
        }
    }
    templateDataStream << "}";

    sendTemplatedEmailRequest.SetTemplateData(templateDataStream.str());

    if (!senderEmailAddress.empty()) {
        sendTemplatedEmailRequest.SetSource(senderEmailAddress);
    }
    if (!replyToAddress.empty()) {
        sendTemplatedEmailRequest.AddReplyToAddresses(replyToAddress);
    }

    auto outcome = sesClient.SendTemplatedEmail(sendTemplatedEmailRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully sent templated message with ID "
                  << outcome.GetResult().GetMessageId()
                  << "." << std::endl;
    }
    else {
        std::cerr << "Error sending templated message. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie SendTemplatedEmailin der AWS SDK für C++ API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sesv2.model.Destination;
import software.amazon.awssdk.services.sesv2.model.EmailContent;
import software.amazon.awssdk.services.sesv2.model.SendEmailRequest;
import software.amazon.awssdk.services.sesv2.model.SesV2Exception;
import software.amazon.awssdk.services.sesv2.SesV2Client;
import software.amazon.awssdk.services.sesv2.model.Template;

/**
 * Before running this AWS SDK for Java (v2) example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * Also, make sure that you create a template. See the following documentation
 * topic:
 *
 * https://docs.aws.amazon.com/ses/latest/dg/send-personalized-email-api.html
 */

public class SendEmailTemplate {
    public static void main(String[] args) {
        final String usage = """
```

```
                Usage:
                    <template> <sender> <recipient>\s

                Where:
                    template - The name of the email template.
                    sender - An email address that represents the sender.\s
                    recipient - An email address that represents the recipient.\s
                """;

        if (args.length != 3) {
            System.out.println(usage);
            System.exit(1);
        }

        String templateName = args[0];
        String sender = args[1];
        String recipient = args[2];
        Region region = Region.US_EAST_1;
        SesV2Client sesv2Client = SesV2Client.builder()
                .region(region)
                .build();

        send(sesv2Client, sender, recipient, templateName);
    }

    public static void send(SesV2Client client, String sender, String recipient,
String templateName) {
        Destination destination = Destination.builder()
                .toAddresses(recipient)
                .build();

        /*
         * Specify both name and favorite animal (favoriteanimal) in your code
when
         * defining the Template object.
         * If you don't specify all the variables in the template, Amazon SES
doesn't
         * send the email.
         */
        Template myTemplate = Template.builder()
                .templateName(templateName)
                .templateData("{\n" +
                        "  \"name\": \"Jason\"\n," +
```

```
                        "  \"favoriteanimal\": \"Cat\"\n" +
                        "}")
                .build();

        EmailContent emailContent = EmailContent.builder()
                .template(myTemplate)
                .build();

        SendEmailRequest emailRequest = SendEmailRequest.builder()
                .destination(destination)
                .content(emailContent)
                .fromEmailAddress(sender)
                .build();

        try {
            System.out.println("Attempting to send an email based on a template
 using the AWS SDK for Java (v2)...");
            client.sendEmail(emailRequest);
            System.out.println("email based on a template was sent");

        } catch (SesV2Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

- Einzelheiten zur API finden Sie SendTemplatedEmailin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { SendTemplatedEmailCommand } from "@aws-sdk/client-ses";
import {
  getUniqueName,
  postfix,
} from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

/**
 * Replace this with the name of an existing template.
 */
const TEMPLATE_NAME = getUniqueName("ReminderTemplate");

/**
 * Replace these with existing verified emails.
 */
const VERIFIED_EMAIL = postfix(getUniqueName("Bilbo"), "@example.com");

const USER = { firstName: "Bilbo", emailAddress: VERIFIED_EMAIL };

/**
 *
 * @param { { emailAddress: string, firstName: string } } user
 * @param { string } templateName - The name of an existing template in Amazon
 SES.
 * @returns { SendTemplatedEmailCommand }
 */
const createReminderEmailCommand = (user, templateName) => {
  return new SendTemplatedEmailCommand({
    /**
     * Here's an example of how a template would be replaced with user data:
     * Template: <h1>Hello {{contact.firstName}},</h1><p>Don't forget about the
 party gifts!</p>
     * Destination: <h1>Hello Bilbo,</h1><p>Don't forget about the party gifts!</
p>
     */
    Destination: { ToAddresses: [user.emailAddress] },
    TemplateData: JSON.stringify({ contact: { firstName: user.firstName } }),
    Source: VERIFIED_EMAIL,
    Template: templateName,
  });
};

const run = async () => {
```

```
  const sendReminderEmailCommand = createReminderEmailCommand(
    USER,
    TEMPLATE_NAME,
  );
  try {
    return await sesClient.send(sendReminderEmailCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
  }
};
```

- Einzelheiten zur API finden Sie SendTemplatedEmailin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesMailSender:
    """Encapsulates functions to send emails with Amazon SES."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def send_templated_email(
```

```
        self, source, destination, template_name, template_data, reply_tos=None
    ):
        """
        Sends an email based on a template. A template contains replaceable tags
        each enclosed in two curly braces, such as {{name}}. The template data
passed
        in this function contains key-value pairs that define the values to
insert
        in place of the template tags.

        Note: If your account is in the Amazon SES  sandbox, the source and
        destination email accounts must both be verified.

        :param source: The source email account.
        :param destination: The destination email account.
        :param template_name: The name of a previously created template.
        :param template_data: JSON-formatted key-value pairs of replacement
values
                              that are inserted in the template before it is
sent.
        :return: The ID of the message, assigned by Amazon SES.
        """
        send_args = {
            "Source": source,
            "Destination": destination.to_service_format(),
            "Template": template_name,
            "TemplateData": json.dumps(template_data),
        }
        if reply_tos is not None:
            send_args["ReplyToAddresses"] = reply_tos
        try:
            response = self.ses_client.send_templated_email(**send_args)
            message_id = response["MessageId"]
            logger.info(
                "Sent templated mail %s from %s to %s.",
                message_id,
                source,
                destination.tos,
            )
        except ClientError:
            logger.exception(
                "Couldn't send templated mail from %s to %s.", source,
destination.tos
            )
```

```
            raise
        else:
            return message_id
```

- Einzelheiten zur API finden Sie SendTemplatedEmailin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    " Send templated email
    DATA(lo_result) = lo_ses->sendtemplatedemail(
      iv_source = iv_source
      io_destination = io_destination
      iv_template = iv_template_name
      iv_templatedata = iv_template_data
      it_replytoaddresses = it_reply_tos
    ).
    ov_msg_id = lo_result->get_messageid( ).
    MESSAGE 'Templated email sent successfully' TYPE 'I'.
  CATCH /aws1/cx_sestmpldoesnotexistex INTO DATA(lo_ex1).
    DATA(lv_error) = |Template does not exist: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex_generic.
ENDTRY.
```

- Einzelheiten zur API finden Sie SendTemplatedEmailin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`UpdateTemplate`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `UpdateTemplate` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Update an Amazon Simple Email Service (Amazon SES) template.
/*!
  \param templateName: The name of the template.
  \param htmlPart: The HTML body of the email.
  \param subjectPart: The subject line of the email.
  \param textPart: The plain text version of the email.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::updateTemplate(const Aws::String &templateName,
                                 const Aws::String &htmlPart,
                                 const Aws::String &subjectPart,
                                 const Aws::String &textPart,
```

```
                                    const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::Template templateValues;

    templateValues.SetTemplateName(templateName);
    templateValues.SetSubjectPart(subjectPart);
    templateValues.SetHtmlPart(htmlPart);
    templateValues.SetTextPart(textPart);

    Aws::SES::Model::UpdateTemplateRequest updateTemplateRequest;
    updateTemplateRequest.SetTemplate(templateValues);

    Aws::SES::Model::UpdateTemplateOutcome outcome =
 sesClient.UpdateTemplate(updateTemplateRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully updated template." << std::endl;
    } else {
        std::cerr << "Error updating template. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie UpdateTemplatein der AWS SDK für C++ API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { UpdateTemplateCommand } from "@aws-sdk/client-ses";
```

```
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const TEMPLATE_NAME = getUniqueName("TemplateName");
const HTML_PART = "<h1>Hello, World!</h1>";

const createUpdateTemplateCommand = () => {
  return new UpdateTemplateCommand({
    Template: {
      TemplateName: TEMPLATE_NAME,
      HtmlPart: HTML_PART,
      SubjectPart: "Example",
      TextPart: "Updated template text.",
    },
  });
};

const run = async () => {
  const updateTemplateCommand = createUpdateTemplateCommand();

  try {
    return await sesClient.send(updateTemplateCommand);
  } catch (err) {
    console.log("Failed to update template.", err);
    return err;
  }
};
```

- Einzelheiten zur API finden Sie UpdateTemplatein der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
 html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def update_template(self, name, subject, text, html):
        """
        Updates a previously created email template.

        :param name: The name of the template.
        :param subject: The subject of the email.
        :param text: The plain text version of the email.
        :param html: The HTML version of the email.
        """
        try:
            template = {
                "TemplateName": name,
                "SubjectPart": subject,
                "TextPart": text,
                "HtmlPart": html,
            }
            self.ses_client.update_template(Template=template)
            logger.info("Updated template %s.", name)
            self.template = template
```

```
            self._extract_tags(subject, text, html)
        except ClientError:
            logger.exception("Couldn't update template %s.", name)
            raise
```

- Einzelheiten zur API finden Sie UpdateTemplatein AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
DATA(lo_template) = NEW /aws1/cl_sestemplate(
  iv_templatename = iv_name
  iv_subjectpart = iv_subject
  iv_textpart = iv_text
  iv_htmlpart = iv_html
).

TRY.
    lo_ses->updatetemplate( io_template = lo_template ).
    MESSAGE 'Template updated successfully' TYPE 'I'.
  CATCH /aws1/cx_sestmpldoesnotexistex INTO DATA(lo_ex1).
    DATA(lv_error) = |Template does not exist: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
  CATCH /aws1/cx_sesinvalidtemplateex INTO DATA(lo_ex2).
    lv_error = |Invalid template: { lo_ex2->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex2.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
```

```
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex_generic.
    ENDTRY.
```

- Einzelheiten zur API finden Sie UpdateTemplatein der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`VerifyDomainIdentity`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `VerifyDomainIdentity` verwendet wird.

Aktionsbeispiele sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Sie können diese Aktion in den folgenden Codebeispielen im Kontext sehen:

- Kopieren von E-Mail- und Domain-Identitäten von Region zu Region
- Amazon Simple Email Service (SES) einrichten
- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

CLI

AWS CLI

So verifizieren Sie eine Domain mit Amazon SES

Im folgenden Beispiel wird der `verify-domain-identity`-Befehl verwendet, um eine Domain zu verifizieren:

```
aws ses verify-domain-identity --domain example.com
```

Ausgabe:

```
{
   "VerificationToken": "eoEmxw+YaYhb3h3iVJHuXMJXqeu1q1/wwmvjuEXAMPLE"
}
```

Um die Domain-Verifizierung abzuschließen, müssen Sie den DNS-Einstellungen Ihrer Domain einen TXT-Eintrag mit dem zurückgegebenen Bestätigungstoken hinzufügen. Weitere Informationen finden Sie unter „Verifizieren von Domains in Amazon SES“ im Entwicklerhandbuch zu Amazon Simple Email Service.

- Einzelheiten zur API finden Sie VerifyDomainIdentityin der AWS CLI Befehlsreferenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import { VerifyDomainIdentityCommand } from "@aws-sdk/client-ses";
import {
  getUniqueName,
  postfix,
} from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

/**
 * You must have access to the domain's DNS settings to complete the
 * domain verification process.
 */
const DOMAIN_NAME = postfix(getUniqueName("Domain"), ".example.com");

const createVerifyDomainIdentityCommand = () => {
  return new VerifyDomainIdentityCommand({ Domain: DOMAIN_NAME });
};

const run = async () => {
  const VerifyDomainIdentityCommand = createVerifyDomainIdentityCommand();

  try {
    return await sesClient.send(VerifyDomainIdentityCommand);
  } catch (err) {
    console.log("Failed to verify domain.", err);
    return err;
```

```
  }
};
```

- Einzelheiten zur API finden Sie VerifyDomainIdentityin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def verify_domain_identity(self, domain_name):
        """
        Starts verification of a domain identity. To complete verification, you
 must
        create a TXT record with a specific format through your DNS provider.

        For more information, see *Verifying a domain with Amazon SES* in the
        Amazon SES documentation:
            https://docs.aws.amazon.com/ses/latest/DeveloperGuide/verify-domain-
procedure.html

        :param domain_name: The name of the domain to verify.
        :return: The token to include in the TXT record with your DNS provider.
        """
```

```
        try:
            response = self.ses_client.verify_domain_identity(Domain=domain_name)
            token = response["VerificationToken"]
            logger.info("Got domain verification token for %s.", domain_name)
        except ClientError:
            logger.exception("Couldn't verify domain %s.", domain_name)
            raise
        else:
            return token
```

- Einzelheiten zur API finden Sie VerifyDomainIdentityin AWS SDK for Python (Boto3) API Reference.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   TRY.
       DATA(lo_result) = lo_ses->verifydomainidentity( iv_domain =
iv_domain_name ).
       ov_token = lo_result->get_verificationtoken( ).
       MESSAGE 'Domain verification initiated' TYPE 'I'.
     CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
       DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
       MESSAGE lv_error TYPE 'I'.
       RAISE EXCEPTION lo_ex.
   ENDTRY.
```

- Einzelheiten zur API finden Sie VerifyDomainIdentityin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`VerifyEmailIdentity`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `VerifyEmailIdentity` verwendet wird.

Aktionsbeispiele sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Sie können diese Aktion in den folgenden Codebeispielen im Kontext sehen:

- Kopieren von E-Mail- und Domain-Identitäten von Region zu Region
- Amazon Simple Email Service (SES) einrichten
- Verifizieren einer E-Mail-Identität und Senden von Nachrichten

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   /// <summary>
   /// Starts verification of an email identity. This request sends an email
   /// from Amazon SES to the specified email address. To complete
   /// verification, follow the instructions in the email.
   /// </summary>
   /// <param name="recipientEmailAddress">Email address to verify.</param>
   /// <returns>True if successful.</returns>
   public async Task<bool> VerifyEmailIdentityAsync(string
recipientEmailAddress)
   {
       var success = false;
       try
       {
           var response = await
_amazonSimpleEmailService.VerifyEmailIdentityAsync(
```

```
                new VerifyEmailIdentityRequest
                {
                    EmailAddress = recipientEmailAddress
                });

            success = response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Exception ex)
        {
            Console.WriteLine("VerifyEmailIdentityAsync failed with exception: "
 + ex.Message);
        }

        return success;
    }
```

- Einzelheiten zur API finden Sie VerifyEmailIdentityin der AWS SDK für .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Add an email address to the list of identities associated with this account
 and
//! initiate verification.
/*!
  \param emailAddress; The email address to add.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::verifyEmailIdentity(const Aws::String &emailAddress,
                         const Aws::Client::ClientConfiguration
 &clientConfiguration)
{
```

```
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::VerifyEmailIdentityRequest verifyEmailIdentityRequest;

    verifyEmailIdentityRequest.SetEmailAddress(emailAddress);

    Aws::SES::Model::VerifyEmailIdentityOutcome outcome =
 sesClient.VerifyEmailIdentity(verifyEmailIdentityRequest);

    if (outcome.IsSuccess())
    {
        std::cout << "Email verification initiated." << std::endl;
    }

    else
    {
        std::cerr << "Error initiating email verification. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie VerifyEmailIdentityin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

So fügen Sie eine E-Mail-Adresse mit Amazon SES hinzu und verifizieren sie

Im folgenden Beispiel wird der `verify-email-identity`-Befehl verwendet, um eine E-Mail-Adresse zu verifizieren:

```
aws ses verify-email-identity --email-address user@example.com
```

Bevor Sie E-Mails mit Amazon SES versenden können, müssen Sie die Adresse oder Domain verifizieren, von denen Sie die E-Mail senden, um zu beweisen, dass sie Ihnen gehören. Ist Sie noch keinen Produktionszugriff haben, müssen Sie außerdem alle E-Mail-

Adresse verifizieren, an die Sie E-Mails senden, mit Ausnahme derer, die vom Amazon-SES-Postfachsimulator bereitgestellt werden.

Nach dem Aufruf verify-email-identity erhält die E-Mail-Adresse eine Bestätigungs-E-Mail. Der Benutzer muss auf den Link in der E-Mail klicken, um den Verifizierungsvorgang abzuschließen.

Weitere Informationen finden Sie unter „Verifizieren von E-Mail-Adressen in Amazon SES“ im Entwicklerhandbuch zu Amazon Simple Email Service.

- Einzelheiten zur API finden Sie VerifyEmailIdentityin der AWS CLI Befehlsreferenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
// Import required AWS SDK clients and commands for Node.js
import { VerifyEmailIdentityCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const EMAIL_ADDRESS = "name@example.com";

const createVerifyEmailIdentityCommand = (emailAddress) => {
  return new VerifyEmailIdentityCommand({ EmailAddress: emailAddress });
};

const run = async () => {
  const verifyEmailIdentityCommand =
    createVerifyEmailIdentityCommand(EMAIL_ADDRESS);
  try {
    return await sesClient.send(verifyEmailIdentityCommand);
  } catch (err) {
    console.log("Failed to verify email identity.", err);
    return err;
  }
```

```
};
```

- Einzelheiten zur API finden Sie VerifyEmailIdentityin der AWS SDK für JavaScript API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def verify_email_identity(self, email_address):
        """
        Starts verification of an email identity. This function causes an email
        to be sent to the specified email address from Amazon SES. To complete
        verification, follow the instructions in the email.

        :param email_address: The email address to verify.
        """
        try:
            self.ses_client.verify_email_identity(EmailAddress=email_address)
            logger.info("Started verification of %s.", email_address)
        except ClientError:
            logger.exception("Couldn't start verification of %s.", email_address)
            raise
```

- Einzelheiten zur API finden Sie VerifyEmailIdentityin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
require 'aws-sdk-ses' # v2: require 'aws-sdk'

# Replace recipient@example.com with a "To" address.
recipient = 'recipient@example.com'

# Create a new SES resource in the us-west-2 region.
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
ses = Aws::SES::Client.new(region: 'us-west-2')

# Try to verify email address.
begin
  ses.verify_email_identity({
                              email_address: recipient
                            })

  puts "Email sent to #{recipient}"

# If something goes wrong, display an error message.
rescue Aws::SES::Errors::ServiceError => e
  puts "Email not sent. Error message: #{e}"
end
```

- Einzelheiten zur API finden Sie VerifyEmailIdentityin der AWS SDK für Ruby API-Referenz.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_ses->verifyemailidentity( iv_emailaddress = iv_email_address ).
    MESSAGE 'Email verification initiated' TYPE 'I'.
  CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.
ENDTRY.
```

- Einzelheiten zur API finden Sie VerifyEmailIdentityin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Szenarien für die Verwendung von Amazon SES AWS SDKs

Die folgenden Codebeispiele zeigen Ihnen, wie Sie gängige Szenarien in Amazon SES mit implementieren AWS SDKs. Diese Szenarien zeigen Ihnen, wie Sie bestimmte Aufgaben durch den Aufruf mehrerer Funktionen innerhalb von Amazon SES oder in Kombination mit anderen AWS-Services ausführen können. Jedes Szenario enthält einen Link zum vollständigen Quell-Code, wo Sie Anleitungen zum Einrichten und Ausführen des Codes finden.

Szenarien zielen auf eine mittlere Erfahrungsebene ab, um Ihnen zu helfen, Service-Aktionen im Kontext zu verstehen.

Beispiele

- Erstellen einer Amazon-Transcribe-Streaming-App
- Kopieren Sie Amazon SES SES-E-Mail- und Domainidentitäten mithilfe eines AWS SDK von einer Region in eine AWS andere
- Erstellen einer Webanwendung zur Verfolgung von DynamoDB-Daten
- Erstellen eines Amazon-Redshift-Element-Trackers
- Erstellen eines Trackers für Aurora-Serverless-Arbeitsaufgaben
- Ermitteln Sie persönliche Schutzausrüstung in Bildern mit Amazon Rekognition mithilfe eines SDK AWS
- Objekte in Bildern mit Amazon Rekognition mithilfe eines SDK erkennen AWS
- Erkennen Sie Personen und Objekte in einem Video mit Amazon Rekognition mithilfe eines SDK AWS
- Generieren von Anmeldeinformationen für die Verbindung mit einem Amazon-SES-SMTP-Endpunkt
- Amazon Simple Email Service (SES) einrichten
- Verwenden von Step Functions, um Lambda-Funktionen aufzurufen
- Überprüfen Sie eine E-Mail-Identität und senden Sie Nachrichten mit Amazon SES mithilfe eines AWS SDK

Erstellen einer Amazon-Transcribe-Streaming-App

Das folgende Code-Beispiel zeigt, wie Sie eine App erstellen, die Live-Audio in Echtzeit aufzeichnet, transkribiert und übersetzt und die Ergebnisse per E-Mail sendet.

JavaScript

SDK für JavaScript (v3)

Zeigt, wie Amazon Transcribe verwendet wird, um eine App zu erstellen, die Live-Audio in Echtzeit aufzeichnet, transkribiert und übersetzt und die Ergebnisse mit Amazon Simple Email Service (Amazon SES) per E-Mail sendet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Comprehend

- Amazon SES
- Amazon Transcribe
- Amazon Translate

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Kopieren Sie Amazon SES SES-E-Mail- und Domainidentitäten mithilfe eines AWS SDK von einer Region in eine AWS andere

Das folgende Codebeispiel zeigt, wie Amazon SES SES-E-Mail- und Domainidentitäten von einer AWS Region in eine andere kopiert werden. Wenn Domänenidentitäten von Route 53 verwaltet werden, werden Überprüfungsdatensätze in die Domäne für die Zielregion kopiert.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import argparse
import json
import logging
from pprint import pprint
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def get_identities(ses_client):
    """
    Gets the identities for the current Region. The Region is specified in the
    Boto3 Amazon SES client object.
```

```
    :param ses_client: A Boto3 Amazon SES client.
    :return: The list of email identities and the list of domain identities.
    """
    email_identities = []
    domain_identities = []
    try:
        identity_paginator = ses_client.get_paginator("list_identities")
        identity_iterator = identity_paginator.paginate(
            PaginationConfig={"PageSize": 20}
        )
        for identity_page in identity_iterator:
            for identity in identity_page["Identities"]:
                if "@" in identity:
                    email_identities.append(identity)
                else:
                    domain_identities.append(identity)
        logger.info(
            "Found %s email and %s domain identities.",
            len(email_identities),
            len(domain_identities),
        )
    except ClientError:
        logger.exception("Couldn't get identities.")
        raise
    else:
        return email_identities, domain_identities


def verify_emails(email_list, ses_client):
    """
    Starts verification of a list of email addresses. Verification causes an
 email
    to be sent to each address. To complete verification, the recipient must
 follow
    the instructions in the email.

    :param email_list: The list of email addresses to verify.
    :param ses_client: A Boto3 Amazon SES client.
    :return: The list of emails that were successfully submitted for
 verification.
    """
    verified_emails = []
    for email in email_list:
        try:
```

```
            ses_client.verify_email_identity(EmailAddress=email)
            verified_emails.append(email)
            logger.info("Started verification of %s.", email)
        except ClientError:
            logger.warning("Couldn't start verification of %s.", email)
    return verified_emails


def verify_domains(domain_list, ses_client):
    """
    Starts verification for a list of domain identities. This returns a token for
    each domain, which must be registered as a TXT record with the DNS provider
 for
    the domain.

    :param domain_list: The list of domains to verify.
    :param ses_client: A Boto3 Amazon SES client.
    :return: The generated domain tokens to use to completed verification.
    """
    domain_tokens = {}
    for domain in domain_list:
        try:
            response = ses_client.verify_domain_identity(Domain=domain)
            token = response["VerificationToken"]
            domain_tokens[domain] = token
            logger.info("Got verification token %s for domain %s.", token,
 domain)
        except ClientError:
            logger.warning("Couldn't get verification token for domain %s.",
 domain)
    return domain_tokens


def get_hosted_zones(route53_client):
    """
    Gets the Amazon Route 53 hosted zones for the current account.

    :param route53_client: A Boto3 Route 53 client.
    :return: The list of hosted zones.
    """
    zones = []
    try:
        zone_paginator = route53_client.get_paginator("list_hosted_zones")
```

```
        zone_iterator = zone_paginator.paginate(PaginationConfig={"PageSize":
 20})
        zones = [
            zone for zone_page in zone_iterator for zone in
 zone_page["HostedZones"]
        ]
        logger.info("Found %s hosted zones.", len(zones))
    except ClientError:
        logger.warning("Couldn't get hosted zones.")
    return zones


def find_domain_zone_matches(domains, zones):
    """
    Finds matches between Amazon SES verified domains and Route 53 hosted zones.
    Subdomain matches are taken when found, otherwise root domain matches are
 taken.

    :param domains: The list of domains to match.
    :param zones: The list of hosted zones to match.
    :return: The set of matched domain-zone pairs. When a match is not found, the
             domain is included in the set with a zone value of None.
    """
    domain_zones = {}
    for domain in domains:
        domain_zones[domain] = None
        # Start at the most specific sub-domain and walk up to the root domain
 until a
        # zone match is found.
        domain_split = domain.split(".")
        for index in range(0, len(domain_split) - 1):
            sub_domain = ".".join(domain_split[index:])
            for zone in zones:
                # Normalize the zone name from Route 53 by removing the trailing
 '.'.
                zone_name = zone["Name"][:-1]
                if sub_domain == zone_name:
                    domain_zones[domain] = zone
                    break
            if domain_zones[domain] is not None:
                break
    return domain_zones
```

```
def add_route53_verification_record(domain, token, zone, route53_client):
    """
    Adds a domain verification TXT record to the specified Route 53 hosted zone.
    When a TXT record already exists in the hosted zone for the specified domain,
    the existing values are preserved and the new token is added to the list.

    :param domain: The domain to add.
    :param token: The verification token for the domain.
    :param zone: The hosted zone where the domain verification record is added.
    :param route53_client: A Boto3 Route 53 client.
    """
    domain_token_record_set_name = f"_amazonses.{domain}"
    record_set_paginator =
 route53_client.get_paginator("list_resource_record_sets")
    record_set_iterator = record_set_paginator.paginate(
        HostedZoneId=zone["Id"], PaginationConfig={"PageSize": 20}
    )
    records = []
    for record_set_page in record_set_iterator:
        try:
            txt_record_set = next(
                record_set
                for record_set in record_set_page["ResourceRecordSets"]
                if record_set["Name"][:-1] == domain_token_record_set_name
                and record_set["Type"] == "TXT"
            )
            records = txt_record_set["ResourceRecords"]
            logger.info(
                "Existing TXT record found in set %s for zone %s.",
                domain_token_record_set_name,
                zone["Name"],
            )
            break
        except StopIteration:
            pass
    records.append({"Value": json.dumps(token)})
    changes = [
        {
            "Action": "UPSERT",
            "ResourceRecordSet": {
                "Name": domain_token_record_set_name,
                "Type": "TXT",
                "TTL": 1800,
                "ResourceRecords": records,
```

```
            },
        }
    ]
    try:
        route53_client.change_resource_record_sets(
            HostedZoneId=zone["Id"], ChangeBatch={"Changes": changes}
        )
        logger.info(
            "Created or updated the TXT record in set %s for zone %s.",
            domain_token_record_set_name,
            zone["Name"],
        )
    except ClientError as err:
        logger.warning(
            "Got error %s. Couldn't create or update the TXT record for zone
 %s.",
            err.response["Error"]["Code"],
            zone["Name"],
        )


def generate_dkim_tokens(domain, ses_client):
    """
    Generates DKIM tokens for a domain. These must be added as CNAME records to
 the
    DNS provider for the domain.

    :param domain: The domain to generate tokens for.
    :param ses_client: A Boto3 Amazon SES client.
    :return: The list of generated DKIM tokens.
    """
    dkim_tokens = []
    try:
        dkim_tokens = ses_client.verify_domain_dkim(Domain=domain)["DkimTokens"]
        logger.info("Generated %s DKIM tokens for domain %s.", len(dkim_tokens),
 domain)
    except ClientError:
        logger.warning("Couldn't generate DKIM tokens for domain %s.", domain)
    return dkim_tokens


def add_dkim_domain_tokens(hosted_zone, domain, tokens, route53_client):
    """
    Adds DKIM domain token CNAME records to a Route 53 hosted zone.
```

```
    :param hosted_zone: The hosted zone where the records are added.
    :param domain: The domain to add.
    :param tokens: The DKIM tokens for the domain to add.
    :param route53_client: A Boto3 Route 53 client.
    """
    try:
        changes = [
            {
                "Action": "UPSERT",
                "ResourceRecordSet": {
                    "Name": f"{token}._domainkey.{domain}",
                    "Type": "CNAME",
                    "TTL": 1800,
                    "ResourceRecords": [{"Value":
 f"{token}.dkim.amazonses.com"}],
                },
            }
            for token in tokens
        ]
        route53_client.change_resource_record_sets(
            HostedZoneId=hosted_zone["Id"], ChangeBatch={"Changes": changes}
        )
        logger.info(
            "Added %s DKIM CNAME records to %s in zone %s.",
            len(tokens),
            domain,
            hosted_zone["Name"],
        )
    except ClientError:
        logger.warning(
            "Couldn't add DKIM CNAME records for %s to zone %s.",
            domain,
            hosted_zone["Name"],
        )


def configure_sns_topics(identity, topics, ses_client):
    """
    Configures Amazon Simple Notification Service (Amazon SNS) notifications for
    an identity. The Amazon SNS topics must already exist.

    :param identity: The identity to configure.
```

```
    :param topics: The list of topics to configure. The choices are Bounce,
 Delivery,
                   or Complaint.
    :param ses_client: A Boto3 Amazon SES client.
    """
    for topic in topics:
        topic_arn = input(
            f"Enter the Amazon Resource Name (ARN) of the {topic} topic or press
 "
            f"Enter to skip: "
        )
        if topic_arn != "":
            try:
                ses_client.set_identity_notification_topic(
                    Identity=identity, NotificationType=topic, SnsTopic=topic_arn
                )
                logger.info("Configured %s for %s notifications.", identity,
 topic)
            except ClientError:
                logger.warning(
                    "Couldn't configure %s for %s notifications.", identity,
 topic
                )


def replicate(source_client, destination_client, route53_client):
    logging.basicConfig(level=logging.INFO, format="%(levelname)s: %(message)s")

    print("-" * 88)
    print(
        f"Replicating Amazon SES identities and other configuration from "
        f"{source_client.meta.region_name} to
 {destination_client.meta.region_name}."
    )
    print("-" * 88)

    print(f"Retrieving identities from {source_client.meta.region_name}.")
    source_emails, source_domains = get_identities(source_client)
    print("Email addresses found:")
    print(*source_emails)
    print("Domains found:")
    print(*source_domains)

    print("Starting verification for email identities.")
```

```
    dest_emails = verify_emails(source_emails, destination_client)
    print("Getting domain tokens for domain identities.")
    dest_domain_tokens = verify_domains(source_domains, destination_client)

    # Get Route 53 hosted zones and match them with Amazon SES domains.
    answer = input(
        "Is the DNS configuration for your domains managed by Amazon Route 53 (y/
n)? "
    )
    use_route53 = answer.lower() == "y"
    hosted_zones = get_hosted_zones(route53_client) if use_route53 else []
    if use_route53:
        print("Adding or updating Route 53 TXT records for your domains.")
        domain_zones = find_domain_zone_matches(dest_domain_tokens.keys(),
 hosted_zones)
        for domain in domain_zones:
            add_route53_verification_record(
                domain, dest_domain_tokens[domain], domain_zones[domain],
 route53_client
            )
    else:
        print(
            "Use these verification tokens to create TXT records through your DNS
 "
            "provider:"
        )
        pprint(dest_domain_tokens)

    answer = input("Do you want to configure DKIM signing for your identities (y/
n)? ")
    if answer.lower() == "y":
        # Build a set of unique domains from email and domain identities.
        domains = {email.split("@")[1] for email in dest_emails}
        domains.update(dest_domain_tokens)
        domain_zones = find_domain_zone_matches(domains, hosted_zones)
        for domain, zone in domain_zones.items():
            answer = input(
                f"Do you want to configure DKIM signing for {domain} (y/n)? "
            )
            if answer.lower() == "y":
                dkim_tokens = generate_dkim_tokens(domain, destination_client)
                if use_route53 and zone is not None:
                    add_dkim_domain_tokens(zone, domain, dkim_tokens,
 route53_client)
```

```
                else:
                    print(
                        "Add the following DKIM tokens as CNAME records through
 your "
                        "DNS provider:"
                    )
                    print(*dkim_tokens, sep="\n")

    answer = input(
        "Do you want to configure Amazon SNS notifications for your identities
 (y/n)? "
    )
    if answer.lower() == "y":
        for identity in dest_emails + list(dest_domain_tokens.keys()):
            answer = input(
                f"Do you want to configure Amazon SNS topics for {identity} (y/
n)? "
            )
            if answer.lower() == "y":
                configure_sns_topics(
                    identity, ["Bounce", "Delivery", "Complaint"],
 destination_client
                )

    print(f"Replication complete for {destination_client.meta.region_name}.")
    print("-" * 88)


def main():
    boto3_session = boto3.Session()
    ses_regions = boto3_session.get_available_regions("ses")
    parser = argparse.ArgumentParser(
        description="Copies email address and domain identities from one AWS
 Region to "
        "another. Optionally adds records for domain verification and DKIM "
        "signing to domains that are managed by Amazon Route 53, "
        "and sets up Amazon SNS notifications for events of interest."
    )
    parser.add_argument(
        "source_region", choices=ses_regions, help="The region to copy from."
    )
    parser.add_argument(
        "destination_region", choices=ses_regions, help="The region to copy to."
    )
```

```
    args = parser.parse_args()
    source_client = boto3.client("ses", region_name=args.source_region)
    destination_client = boto3.client("ses", region_name=args.destination_region)
    route53_client = boto3.client("route53")
    replicate(source_client, destination_client, route53_client)


if __name__ == "__main__":
    main()
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Python (Boto3).
  - ListIdentities
  - SetIdentityNotificationTopic
  - VerifyDomainDkim
  - VerifyDomainIdentity
  - VerifyEmailIdentity

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen einer Webanwendung zur Verfolgung von DynamoDB-Daten

Die folgenden Code-Beispiele zeigen, wie eine Webanwendung erstellt wird, die Arbeitselemente in einer Amazon DynamoDB-Tabelle verfolgt und mithilfe von Amazon Simple Email Service (Amazon SES) Berichte sendet.

.NET

SDK für .NET

Zeigt, wie man die Amazon-DynamoDB-.NET-API verwendet, um eine dynamische Webanwendung zu erstellen, die DynamoDB-Arbeitsdaten verfolgt.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Amazon SES

Java

SDK für Java 2.x

Zeigt, wie man die Amazon-DynamoDB-API verwendet, um eine dynamische Webanwendung zu erstellen, die DynamoDB-Arbeitsdaten verfolgt.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Amazon SES

Kotlin

SDK für Kotlin

Zeigt, wie man die Amazon-DynamoDB-API verwendet, um eine dynamische Webanwendung zu erstellen, die DynamoDB-Arbeitsdaten verfolgt.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Amazon SES

Python

SDK für Python (Boto3)

Zeigt, wie Sie mithilfe von Amazon Simple Email Service (Amazon SES) einen REST-Service erstellen, der Arbeitselemente in Amazon DynamoDB nachverfolgt und Berichte

per E-Mail versendet. AWS SDK für Python (Boto3) In diesem Beispiel wird das Flask-Web-Framework für das HTTP-Routing verwendet und in eine React-Webseite integriert, um eine voll funktionsfähige Webanwendung zu präsentieren.

- Erstellen Sie einen Flask-REST-Service, der sich in integrieren lässt. AWS-Services
- Lesen, schreiben und aktualisieren Sie Arbeitsaufgaben, die in einer DynamoDB-Tabelle gespeichert sind.
- Verwenden Sie Amazon SES, um E-Mail-Berichte über Arbeitsaufgaben zu senden.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel im AWS Code Examples Repository unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Amazon SES

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen eines Amazon-Redshift-Element-Trackers

Die folgenden Code-Beispiele zeigen, wie Sie eine Webanwendung erstellen, die Arbeitselemente mit einer Amazon-Redshift-Datenbank verfolgt und darüber berichtet.

Java

SDK für Java 2.x

Zeigt, wie eine Webanwendung erstellt wird, die in einer Amazon-Redshift-Datenbank gespeicherte Arbeitselemente verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer Spring REST-API, die Amazon Redshift Redshift-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Redshift

- Amazon SES

Kotlin

SDK für Kotlin

Zeigt, wie eine Webanwendung erstellt wird, die in einer Amazon-Redshift-Datenbank gespeicherte Arbeitselemente verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer Spring REST-API, die Amazon Redshift Redshift-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Redshift
- Amazon SES

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen eines Trackers für Aurora-Serverless-Arbeitsaufgaben

Die folgenden Code-Beispiele zeigen, wie eine Webanwendung erstellt wird, die Arbeitselemente in einer Amazon Aurora Serverless-Datenbank verfolgt und mithilfe von Amazon Simple Email Service (Amazon SES) Berichte sendet.

.NET

SDK für .NET

Zeigt, wie Sie mithilfe von Amazon Simple Email Service (Amazon SES) eine Webanwendung erstellen, die Arbeitsaufgaben in einer Amazon Aurora Aurora-Datenbank nachverfolgt und Berichte per E-Mail versendet. AWS SDK für .NET In diesem Beispiel wird ein mit React.js erstelltes Frontend verwendet, um mit RESTful einem.NET-Backend zu interagieren.

- Integrieren Sie eine React-Webanwendung in AWS Dienste.
- Auflisten, Hinzufügen, Aktualisieren und Löschen von Elementen in einer Aurora-Tabelle.

- Senden Sie einen E-Mail-Bericht über gefilterte Arbeitselemente mit Amazon SES.
- Stellen Sie Beispielressourcen mit dem mitgelieferten AWS CloudFormation Skript bereit und verwalten Sie sie.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

C++

SDK für C++

Zeigt, wie eine Webanwendung erstellt wird, die in einer Datenbank von Amazon Aurora Serverless gespeicherte Arbeitselemente verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer C++-REST-API, die Amazon Aurora Aurora-Serverless-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

Java

SDK für Java 2.x

Zeigt, wie eine Webanwendung erstellt wird, die Arbeitselemente, die in einer Amazon RDS-Datenbank gespeichert sind, verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer Spring REST-API, die Amazon Aurora Aurora-Serverless-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

Den vollständigen Quellcode und Anweisungen zum Einrichten und Ausführen eines Beispiels, das die JDBC-API verwendet, finden Sie im vollständigen Beispiel unter. GitHub

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

JavaScript

SDK für JavaScript (v3)

Zeigt, wie Sie mit AWS SDK für JavaScript (v3) eine Webanwendung erstellen, die Arbeitsaufgaben in einer Amazon Aurora Aurora-Datenbank verfolgt und Berichte mithilfe von Amazon Simple Email Service (Amazon SES) per E-Mail versendet. In diesem Beispiel wird ein mit React.js erstelltes Frontend verwendet, um mit einem Express-Node.js-Backend zu interagieren.

- Integrieren Sie eine React.js Webanwendung mit AWS-Services.
- Auflisten, hinzufügen und aktualisieren von Elementen in einer Aurora-Tabelle.
- Senden Sie einen E-Mail-Bericht über gefilterte Arbeitselemente mit Amazon SES.
- Stellen Sie Beispielressourcen mit dem mitgelieferten AWS CloudFormation Skript bereit und verwalten Sie sie.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

Kotlin

SDK für Kotlin

Zeigt, wie eine Webanwendung erstellt wird, die Arbeitselemente, die in einer Amazon RDS-Datenbank gespeichert sind, verfolgt und darüber berichtet.

Den vollständigen Quellcode und Anweisungen zur Einrichtung einer Spring REST-API, die Amazon Aurora Aurora-Serverless-Daten abfragt und von einer React-Anwendung verwendet werden kann, finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

PHP

SDK für PHP

Zeigt, wie Sie mithilfe von Amazon Simple Email Service (Amazon SES) eine Webanwendung erstellen, die Arbeitselemente in einer Amazon RDS-Datenbank verfolgt und Berichte per E-Mail versendet. AWS SDK für PHP In diesem Beispiel wird ein mit React.js erstelltes Frontend verwendet, um mit einem RESTful PHP-Backend zu interagieren.

- Integrieren Sie eine React.js -Webanwendung in AWS Dienste.
- In einer Amazon-RDS-Tabelle können Sie Elemente auflisten, aktualisieren und löschen.
- Senden Sie einen E-Mail-Bericht über gefilterte Arbeitselemente mit Amazon SES.
- Stellen Sie Beispielressourcen mit dem mitgelieferten AWS CloudFormation Skript bereit und verwalten Sie sie.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora

- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

Python

SDK für Python (Boto3)

Zeigt, wie Sie mithilfe von Amazon Simple Email Service (Amazon SES) einen REST-Service erstellen, der Arbeitselemente in einer Amazon Aurora Aurora-Serverless-Datenbank nachverfolgt und Berichte per E-Mail versendet. AWS SDK für Python (Boto3) In diesem Beispiel wird das Flask-Web-Framework für das HTTP-Routing verwendet und in eine React-Webseite integriert, um eine voll funktionsfähige Webanwendung zu präsentieren.

- Erstellen Sie einen Flask-REST-Service, der sich in integrieren lässt. AWS-Services
- Lesen, schreiben und aktualisieren Sie Arbeitsaufgaben, die in einer Aurora-Serverless-Datenbank gespeichert sind.
- Erstellen Sie ein AWS Secrets Manager Geheimnis, das Datenbankanmeldedaten enthält, und verwenden Sie es, um Aufrufe an die Datenbank zu authentifizieren.
- Verwenden Sie Amazon SES, um E-Mail-Berichte über Arbeitsaufgaben zu senden.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Aurora
- Amazon RDS
- Amazon RDS Data Service
- Amazon SES

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Ermitteln Sie persönliche Schutzausrüstung in Bildern mit Amazon Rekognition mithilfe eines SDK AWS

Das folgende Codebeispiel zeigt, wie eine App erstellt wird, die Amazon Rekognition verwendet, um persönliche Schutzausrüstung (PSA) auf Bildern zu erkennen.

Java

SDK für Java 2.x

Zeigt, wie eine AWS Lambda Funktion erstellt wird, die Bilder mit persönlicher Schutzausrüstung erkennt.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Amazon Rekognition
- Amazon S3
- Amazon SES

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Objekte in Bildern mit Amazon Rekognition mithilfe eines SDK erkennen AWS

Die folgenden Code-Beispiele zeigen, wie man eine App erstellt, die Amazon Rekognition verwendet, um Objekte nach Kategorien in Bildern zu erkennen.

.NET

SDK für .NET

Zeigt, wie Sie die Amazon-Rekognition-.NET-API verwenden, um eine App zu erstellen, die Amazon Rekognition verwendet, um Objekte nach Kategorien in Bildern zu identifizieren, die sich in einem Bucket von Amazon Simple Storage Service (Amazon S3) befinden. Die App

sendet dem Administrator eine E-Mail-Benachrichtigung mit den Ergebnissen über Amazon Simple Email Service (Amazon SES).

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Rekognition
- Amazon S3
- Amazon SES

Java

SDK für Java 2.x

Zeigt, wie man die Amazon-Rekognition-Java-API verwendet, um eine App zu erstellen, die Amazon Rekognition verwendet, um Objekte nach Kategorien in Bildern zu identifizieren, die sich in einem Amazon Simple Storage Service (Amazon S3)-Bucket befinden. Die App sendet dem Administrator eine E-Mail-Benachrichtigung mit den Ergebnissen über Amazon Simple Email Service (Amazon SES).

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK für JavaScript (v3)

Zeigt, wie Amazon Rekognition zusammen mit dem verwendet wird, um eine App AWS SDK für JavaScript zu erstellen, die Amazon Rekognition verwendet, um Objekte nach Kategorien in Bildern zu identifizieren, die sich in einem Amazon Simple Storage Service (Amazon S3)

-Bucket befinden. Die App sendet dem Administrator eine E-Mail-Benachrichtigung mit den Ergebnissen über Amazon Simple Email Service (Amazon SES).

Lernen Sie Folgendes:

- Erstellen Sie mit Amazon Cognito einen nicht authentifizierten Benutzer.
- Analysieren Sie mit Amazon Rekognition Bilder für Objekte.
- Verifizieren Sie eine E-Mail-Adresse für Amazon SES.
- Senden Sie eine E-Mail-Benachrichtigung mit Amazon SES.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter. GitHub

In diesem Beispiel verwendete Dienste

- Amazon Rekognition
- Amazon S3
- Amazon SES

Kotlin

SDK für Kotlin

Zeigt, wie man die Amazon-Rekognition-Kotlin-API verwendet, um eine App zu erstellen, die Amazon Rekognition verwendet, um Objekte nach Kategorien in Bildern zu identifizieren, die sich in einem Amazon Simple Storage Service (Amazon S3)-Bucket befinden. Die App sendet dem Administrator eine E-Mail-Benachrichtigung mit den Ergebnissen über Amazon Simple Email Service (Amazon SES).

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Rekognition
- Amazon S3
- Amazon SES

Python

SDK für Python (Boto3)

Zeigt Ihnen, wie Sie mit AWS SDK für Python (Boto3) dem eine Webanwendung erstellen, mit der Sie Folgendes tun können:

- Laden Sie Fotos in einen Bucket von Amazon Simple Storage Service (Amazon S3) hoch.
- Verwenden Sie Amazon Rekognition, um die Fotos zu analysieren und zu markieren.
- Verwenden Sie Amazon Simple Email Service (Amazon SES), um E-Mail-Berichte von Bildanalysen zu senden.

Dieses Beispiel enthält zwei Hauptkomponenten: eine eingeschriebene Webseite JavaScript , die mit React erstellt wurde, und einen in Python geschriebenen REST-Dienst, der mit Flask-RESTful erstellt wurde.

Sie können die React-Webseite verwenden, um Folgendes auszuführen:

- Zeigen Sie eine Liste der Bilder an, die in Ihrem S3-Bucket gespeichert sind.
- Laden Sie Bilder von Ihrem Computer in Ihren S3-Bucket hoch.
- Zeigen Sie Bilder und Markierungen an, die Elemente identifizieren, welche im Bild erkannt werden.
- Rufen Sie einen Bericht über alle Bilder in Ihrem S3-Bucket ab und senden Sie eine E-Mail mit dem Bericht.

Die Webseite ruft den REST-Service auf. Der Service sendet Anforderungen an AWS , um die folgenden Aktionen durchzuführen:

- Die Liste der Bilder abrufen und in Ihrem S3-Bucket filtern.
- Fotos in Ihren S3-Bucket hochladen.
- Verwenden Sie Amazon Rekognition, um einzelne Fotos zu analysieren und eine Liste von Markierungen zu erhalten, die die auf dem Foto erkannten Elemente identifizieren.
- Analysieren Sie alle Fotos in Ihrem S3-Bucket und verwenden Sie Amazon SES, um einen Bericht per E-Mail zu senden.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Rekognition

- Amazon S3
- Amazon SES

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erkennen Sie Personen und Objekte in einem Video mit Amazon Rekognition mithilfe eines SDK AWS

Die folgenden Code-Beispiele zeigen, wie man Personen und Objekte in einem Video mit Amazon Rekognition erkennt.

Java

SDK für Java 2.x

Zeigt, wie man die Amazon-Rekognition-Java-API verwendet, um eine App zu erstellen, die Gesichter und Objekte in Videos erkennt, die sich in einem Amazon Simple Storage Service (Amazon S3)-Bucket befinden. Die App sendet dem Administrator eine E-Mail-Benachrichtigung mit den Ergebnissen über Amazon Simple Email Service (Amazon SES).

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Rekognition
- Amazon S3
- Amazon SES
- Amazon SNS
- Amazon SQS

Python

SDK für Python (Boto3)

Verwenden Sie Amazon Rekognition, um Gesichter, Objekte und Personen in Videos zu erkennen, indem Sie asynchrone Erkennungsaufträge starten. In diesem Beispiel wird

Amazon Rekognition auch so konfiguriert, dass es ein Amazon Simple Notification Service (Amazon SNS)-Thema benachrichtigt, wenn Aufträge abgeschlossen sind, und eine Amazon Simple Queue Service (Amazon SQS)-Warteschlange bei dem Thema abonniert. Wenn die Warteschlange eine Meldung über einen Job erhält, wird der Job abgerufen und die Ergebnisse werden ausgegeben.

Dieses Beispiel lässt sich am besten auf ansehen GitHub. Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Rekognition
- Amazon S3
- Amazon SES
- Amazon SNS
- Amazon SQS

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Generieren von Anmeldeinformationen für die Verbindung mit einem Amazon-SES-SMTP-Endpunkt

Das folgende Code-Beispiel zeigt, wie Sie Anmeldeinformationen erzeugen, um eine Verbindung mit einem Amazon-SES-SMTP-Endpunkt herzustellen.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
#!/usr/bin/env python3
```

```
import hmac
import hashlib
import base64
import argparse

SMTP_REGIONS = [
    "us-east-2",  # US East (Ohio)
    "us-east-1",  # US East (N. Virginia)
    "us-west-2",  # US West (Oregon)
    "ap-south-1",  # Asia Pacific (Mumbai)
    "ap-northeast-2",  # Asia Pacific (Seoul)
    "ap-southeast-1",  # Asia Pacific (Singapore)
    "ap-southeast-2",  # Asia Pacific (Sydney)
    "ap-northeast-1",  # Asia Pacific (Tokyo)
    "ca-central-1",  # Canada (Central)
    "eu-central-1",  # Europe (Frankfurt)
    "eu-west-1",  # Europe (Ireland)
    "eu-west-2",  # Europe (London)
    "eu-south-1",  # Europe (Milan)
    "eu-north-1",  # Europe (Stockholm)
    "sa-east-1",  # South America (Sao Paulo)
    "us-gov-west-1",  # AWS GovCloud (US)
    "us-gov-east-1",  # AWS GovCloud (US)
]

# These values are required to calculate the signature. Do not change them.
DATE = "11111111"
SERVICE = "ses"
MESSAGE = "SendRawEmail"
TERMINAL = "aws4_request"
VERSION = 0x04


def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()


def calculate_key(secret_access_key, region):
    if region not in SMTP_REGIONS:
        raise ValueError(f"The {region} Region doesn't have an SMTP endpoint.")

    signature = sign(("AWS4" + secret_access_key).encode("utf-8"), DATE)
    signature = sign(signature, region)
```

```
    signature = sign(signature, SERVICE)
    signature = sign(signature, TERMINAL)
    signature = sign(signature, MESSAGE)
    signature_and_version = bytes([VERSION]) + signature
    smtp_password = base64.b64encode(signature_and_version)
    return smtp_password.decode("utf-8")


def main():
    parser = argparse.ArgumentParser(
        description="Convert a Secret Access Key to an SMTP password."
    )
    parser.add_argument("secret", help="The Secret Access Key to convert.")
    parser.add_argument(
        "region",
        help="The AWS Region where the SMTP password will be used.",
        choices=SMTP_REGIONS,
    )
    args = parser.parse_args()
    print(calculate_key(args.secret, args.region))


if __name__ == "__main__":
    main()
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Amazon Simple Email Service (SES) einrichten

Wie das aussehen kann, sehen Sie am nachfolgenden Beispielcode:

- Verifizieren Sie eine E-Mail-Adresse
- Verifizieren Sie eine Domain (optional)
- Überprüfe deine Sendelimits
- Senden Sie eine Test-E-Mail
- Bereinigen von Ressourcen

Bash

AWS CLI mit Bash-Skript

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie es im Tutorials und Beispiele-Repository für Entwickler einrichten und ausführen.

```
#!/bin/bash

# Amazon SES Setup Script (v2)
# This script helps you set up Amazon SES for sending emails

# Initialize log file
LOG_FILE="ses-setup.log"
echo "Starting Amazon SES setup at $(date)" > "$LOG_FILE"

# Function to log commands and their output
log_cmd() {
    echo "Running: $1" | tee -a "$LOG_FILE"
    eval "$1" 2>&1 | tee -a "$LOG_FILE"
    return ${PIPESTATUS[0]}
}

# Function to check for errors in command output
check_error() {
    local cmd_output="$1"
    local cmd_status="$2"
    local error_msg="$3"
    local ignore_error="${4:-false}"

    if [[ $cmd_status -ne 0 || "$cmd_output" =~ [Ee][Rr][Rr][Oo][Rr] ]]; then
        echo "ERROR: $error_msg" | tee -a "$LOG_FILE"
        if [[ "$ignore_error" != "true" ]]; then
            cleanup_resources
            exit 1
        fi
    fi
}
```

```
# Function to clean up resources
cleanup_resources() {
    echo "Cleaning up resources..." | tee -a "$LOG_FILE"

    # No physical resources to clean up for SES setup
    # Email identities can be deleted if needed
    if [[ -n "$EMAIL_ADDRESS" ]]; then
        echo "Deleting email identity: $EMAIL_ADDRESS" | tee -a "$LOG_FILE"
        log_cmd "aws ses delete-identity --identity \"$EMAIL_ADDRESS\""
    fi

    if [[ -n "$RECIPIENT_EMAIL" && "$RECIPIENT_EMAIL" != "$EMAIL_ADDRESS" ]];
 then
        echo "Deleting recipient email identity: $RECIPIENT_EMAIL" | tee -a
 "$LOG_FILE"
        log_cmd "aws ses delete-identity --identity \"$RECIPIENT_EMAIL\""
    fi

    if [[ -n "$DOMAIN_NAME" ]]; then
        echo "Deleting domain identity: $DOMAIN_NAME" | tee -a "$LOG_FILE"
        log_cmd "aws ses delete-identity --identity \"$DOMAIN_NAME\""
    fi
}

# Track created resources
CREATED_RESOURCES=()

# Welcome message
echo "============================================="
echo "Amazon SES Setup Script"
echo "============================================="
echo "This script will help you set up Amazon SES for sending emails."
echo "You'll need to verify at least one email address that you own."
echo ""
echo "NOTE: New SES accounts are placed in the sandbox environment."
echo "In the sandbox, both sender AND recipient email addresses must be
 verified."
echo ""

# Get email address to verify
echo "Please enter an email address that you own and can access:"
read -r EMAIL_ADDRESS
```

```
# Verify email identity
echo "Verifying email address: $EMAIL_ADDRESS" | tee -a "$LOG_FILE"
OUTPUT=$(log_cmd "aws ses verify-email-identity --email-address \"$EMAIL_ADDRESS
\"")
check_error "$OUTPUT" $? "Failed to verify email address"

CREATED_RESOURCES+=("Email identity: $EMAIL_ADDRESS")
echo "A verification email has been sent to $EMAIL_ADDRESS."
echo "Please check your inbox and click the verification link before continuing."
echo ""
echo "Press Enter after you've verified your email address..."
read -r

# Check verification status
echo "Checking verification status..." | tee -a "$LOG_FILE"
OUTPUT=$(log_cmd "aws ses list-identities --identity-type EmailAddress")
check_error "$OUTPUT" $? "Failed to list identities"

OUTPUT=$(log_cmd "aws ses get-identity-verification-attributes --identities
 \"$EMAIL_ADDRESS\"")
check_error "$OUTPUT" $? "Failed to get verification attributes"

# Check if the email is verified
VERIFICATION_STATUS=$(echo "$OUTPUT" | grep -o '"VerificationStatus": "[^"]*' |
 cut -d'"' -f4)
if [[ "$VERIFICATION_STATUS" != "Success" ]]; then
    echo "Email address $EMAIL_ADDRESS is not verified yet. Please check your
 inbox and verify before continuing."
    echo "Exiting script..."
    exit 1
fi

# Ask if user wants to verify a domain
echo ""
echo "Do you want to verify a domain for sending emails? (y/n):"
read -r VERIFY_DOMAIN

if [[ "$VERIFY_DOMAIN" =~ ^[Yy] ]]; then
    echo "Please enter the domain name you want to verify:"
    read -r DOMAIN_NAME

    # Verify domain identity
    echo "Verifying domain: $DOMAIN_NAME" | tee -a "$LOG_FILE"
    OUTPUT=$(log_cmd "aws ses verify-domain-identity --domain \"$DOMAIN_NAME\"")
```

```
    check_error "$OUTPUT" $? "Failed to verify domain identity"

    # Extract verification token
    VERIFICATION_TOKEN=$(echo "$OUTPUT" | grep -o '"VerificationToken": "[^"]*' |
cut -d'"' -f4)

    CREATED_RESOURCES+=("Domain identity: $DOMAIN_NAME")

    echo ""
    echo "============================================="
    echo "Domain Verification Instructions"
    echo "============================================="
    echo "To verify your domain ownership, you need to add a TXT record"
    echo "to your domain's DNS settings with the following values:"
    echo ""
    echo "Record Type: TXT"
    echo "Record Name: _amazonses.$DOMAIN_NAME"
    echo "Record Value: $VERIFICATION_TOKEN"
    echo ""
    echo "After adding this DNS record, verification may take up to 72 hours."
    echo ""

    # Set up DKIM for the domain
    echo "Setting up DKIM for domain: $DOMAIN_NAME" | tee -a "$LOG_FILE"
    OUTPUT=$(log_cmd "aws ses verify-domain-dkim --domain \"$DOMAIN_NAME\"")
    check_error "$OUTPUT" $? "Failed to set up DKIM"

    # Extract DKIM tokens
    DKIM_TOKENS=$(echo "$OUTPUT" | grep -o '"DkimTokens": \[[^]]*\]' | sed
's/"DkimTokens": \[\|\]//g' | sed 's/,//g' | sed 's/"//g')

    echo "============================================="
    echo "DKIM Configuration Instructions"
    echo "============================================="
    echo "To configure DKIM for your domain, add the following CNAME records"
    echo "to your domain's DNS settings:"
    echo ""

    for token in $DKIM_TOKENS; do
        echo "Record Type: CNAME"
        echo "Record Name: ${token}._domainkey.$DOMAIN_NAME"
        echo "Record Value: ${token}.dkim.amazonses.com"
        echo ""
    done
```

```
    echo "After adding these DNS records, DKIM verification may take up to 72
 hours."
    echo ""
fi

# Check sending limits
echo "Checking your SES sending limits..." | tee -a "$LOG_FILE"
OUTPUT=$(log_cmd "aws ses get-send-quota")
check_error "$OUTPUT" $? "Failed to get sending quota"

# Extract quota information
MAX_SEND_RATE=$(echo "$OUTPUT" | grep -o '"MaxSendRate": [0-9.]*' | cut -d' ' -
f2)
MAX_24_HOUR_SEND=$(echo "$OUTPUT" | grep -o '"Max24HourSend": [0-9.]*' | cut -d'
 ' -f2)
SENT_LAST_24_HOURS=$(echo "$OUTPUT" | grep -o '"SentLast24Hours": [0-9.]*' | cut
 -d' ' -f2)

echo ""
echo "============================================="
echo "Your SES Sending Limits"
echo "============================================="
echo "Maximum send rate: $MAX_SEND_RATE emails/second"
echo "Maximum 24-hour send: $MAX_24_HOUR_SEND emails"
echo "Sent in the last 24 hours: $SENT_LAST_24_HOURS emails"
echo ""

# Ask if user wants to send a test email
echo "Do you want to send a test email? (y/n):"
read -r SEND_TEST

if [[ "$SEND_TEST" =~ ^[Yy] ]]; then
    echo ""
    echo "============================================="
    echo "SANDBOX ENVIRONMENT NOTICE"
    echo "============================================="
    echo "Your account is likely in the SES sandbox environment."
    echo "In the sandbox, you can only send emails to verified email addresses."
    echo ""
    echo "Do you want to:"
    echo "1. Send a test email to the same verified address ($EMAIL_ADDRESS)"
    echo "2. Verify another email address to use as recipient"
    echo ""
```

```
    echo "Enter your choice (1 or 2):"
    read -r RECIPIENT_CHOICE

    if [[ "$RECIPIENT_CHOICE" == "1" ]]; then
        RECIPIENT_EMAIL="$EMAIL_ADDRESS"
    else
        echo "Please enter the recipient email address you want to verify:"
        read -r RECIPIENT_EMAIL

        # Verify recipient email identity if different from sender
        if [[ "$RECIPIENT_EMAIL" != "$EMAIL_ADDRESS" ]]; then
            echo "Verifying recipient email address: $RECIPIENT_EMAIL" | tee -a
 "$LOG_FILE"
            OUTPUT=$(log_cmd "aws ses verify-email-identity --email-address
 \"$RECIPIENT_EMAIL\"")
            check_error "$OUTPUT" $? "Failed to verify recipient email address"

            CREATED_RESOURCES+=("Email identity: $RECIPIENT_EMAIL")
            echo "A verification email has been sent to $RECIPIENT_EMAIL."
            echo "Please check the inbox and click the verification link before
 continuing."
            echo ""
            echo "Press Enter after you've verified the recipient email
 address..."
            read -r

            # Check recipient verification status
            OUTPUT=$(log_cmd "aws ses get-identity-verification-attributes --
identities \"$RECIPIENT_EMAIL\"")
            check_error "$OUTPUT" $? "Failed to get recipient verification
 attributes"

            # Check if the recipient email is verified
            RECIPIENT_VERIFICATION_STATUS=$(echo "$OUTPUT" | grep -o
 '"VerificationStatus": "[^"]*' | cut -d'"' -f4)
            if [[ "$RECIPIENT_VERIFICATION_STATUS" != "Success" ]]; then
                echo "Recipient email address $RECIPIENT_EMAIL is not verified
 yet."
                echo "You can try sending the email anyway, but it may fail."
            fi
        fi
    fi
```

```
    echo "Sending test email from $EMAIL_ADDRESS to $RECIPIENT_EMAIL..." | tee -a
 "$LOG_FILE"
    OUTPUT=$(log_cmd "aws ses send-email \
        --from \"$EMAIL_ADDRESS\" \
        --destination \"ToAddresses=$RECIPIENT_EMAIL\" \
        --message \"Subject={Data=SES Test
 Email,Charset=UTF-8},Body={Text={Data=This is a test email sent from Amazon SES
 using the AWS CLI,Charset=UTF-8}}\"")

    # Don't exit on send email error, just report it
    check_error "$OUTPUT" $? "Failed to send test email" "true"

    # Check if the email was sent successfully
    if [[ "$OUTPUT" =~ "MessageId" ]]; then
        # Extract message ID
        MESSAGE_ID=$(echo "$OUTPUT" | grep -o '"MessageId": "[^"]*' | cut -d'"' -
f4)
        echo "Test email sent successfully! Message ID: $MESSAGE_ID"
    else
        echo "Failed to send test email. This is likely because your account is
 in the sandbox environment."
        echo "In the sandbox, both sender AND recipient email addresses must be
 verified."
    fi
    echo ""
fi

# Summary of created resources
echo ""
echo "============================================="
echo "Setup Complete - Resources Created"
echo "============================================="
for resource in "${CREATED_RESOURCES[@]}"; do
    echo "- $resource"
done
echo ""

# Ask if user wants to clean up resources
echo "============================================="
echo "CLEANUP CONFIRMATION"
echo "============================================="
echo "Do you want to clean up all created resources? (y/n):"
read -r CLEANUP_CHOICE
```

```
if [[ "$CLEANUP_CHOICE" =~ ^[Yy] ]]; then
    cleanup_resources
    echo "Cleanup completed."
else
    echo "Resources have been preserved."
fi

echo ""
echo "============================================="
echo "Amazon SES Setup Complete"
echo "============================================="
echo "For production use, you may need to request to be moved out of the SES
 sandbox."
echo "Visit the SES console and navigate to 'Account dashboard' to request
 production access."
echo ""
echo "Log file: $LOG_FILE"
echo "============================================="
```

- Weitere API-Informationen finden Sie in den folgenden Themen der AWS CLI - Befehlsreferenz.
  - DeleteIdentity
  - GetIdentityVerificationAttributes
  - GetSendQuota
  - ListIdentities
  - SendEmail
  - VerifyDomainDkim
  - VerifyDomainIdentity
  - VerifyEmailIdentity

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwenden von Step Functions, um Lambda-Funktionen aufzurufen

Das folgende Codebeispiel zeigt, wie Sie eine AWS Step Functions Zustandsmaschine erstellen, die nacheinander AWS Lambda Funktionen aufruft.

Java

SDK für Java 2.x

Zeigt, wie Sie mithilfe von AWS Step Functions und einen AWS serverlosen Workflow erstellen. AWS SDK for Java 2.x Jeder Workflow-Schritt wird mithilfe einer AWS Lambda Funktion implementiert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Überprüfen Sie eine E-Mail-Identität und senden Sie Nachrichten mit Amazon SES mithilfe eines AWS SDK

Wie das aussehen kann, sehen Sie am nachfolgenden Beispielcode:

- Hinzufügen und verifizieren einer E-Mail-Adresse mit Amazon SES.
- Senden einer standardmäßigen E-Mail-Nachricht.
- Erstellen Sie eine Vorlage und senden Sie eine E-Mail-Nachricht mit Vorlage.
- Senden einer Nachricht mithilfe eines Amazon-SES-SMTP-Servers.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Verifizieren einer E-Mail-Adresse mit Amazon SES und senden von Nachrichten.

```
def usage_demo():
    print("-" * 88)
    print("Welcome to the Amazon Simple Email Service (Amazon SES) email demo!")
    print("-" * 88)

    logging.basicConfig(level=logging.INFO, format="%(levelname)s: %(message)s")

    ses_client = boto3.client("ses")
    ses_identity = SesIdentity(ses_client)
    ses_mail_sender = SesMailSender(ses_client)
    ses_template = SesTemplate(ses_client)
    email = input("Enter an email address to send mail with Amazon SES: ")
    status = ses_identity.get_identity_status(email)
    verified = status == "Success"
    if not verified:
        answer = input(
            f"The address '{email}' is not verified with Amazon SES. Unless your
 "
            f"Amazon SES account is out of sandbox, you can send mail only from "
            f"and to verified accounts. Do you want to verify this account for
 use "
            f"with Amazon SES? If yes, the address will receive a verification "
            f"email (y/n): "
        )
        if answer.lower() == "y":
            ses_identity.verify_email_identity(email)
            print(f"Follow the steps in the email to {email} to complete
 verification.")
            print("Waiting for verification...")
            try:
                ses_identity.wait_until_identity_exists(email)
```

```
                print(f"Identity verified for {email}.")
                verified = True
            except WaiterError:
                print(
                    f"Verification timeout exceeded. You must complete the "
                    f"steps in the email sent to {email} to verify the address."
                )

    if verified:
        test_message_text = "Hello from the Amazon SES mail demo!"
        test_message_html = "<p>Hello!</p><p>From the <b>Amazon SES</b> mail
demo!</p>"

        print(f"Sending mail from {email} to {email}.")
        ses_mail_sender.send_email(
            email,
            SesDestination([email]),
            "Amazon SES demo",
            test_message_text,
            test_message_html,
        )
        input("Mail sent. Check your inbox and press Enter to continue.")

        template = {
            "name": "doc-example-template",
            "subject": "Example of an email template.",
            "text": "This is what {{name}} will {{action}} if {{name}} can't
display "
            "HTML.",
            "html": "<p><i>This</i> is what {{name}} will {{action}} if {{name}}
"
            "<b>can</b> display HTML.</p>",
        }
        print("Creating a template and sending a templated email.")
        ses_template.create_template(**template)
        template_data = {"name": email.split("@")[0], "action": "read"}
        if ses_template.verify_tags(template_data):
            ses_mail_sender.send_templated_email(
                email, SesDestination([email]), ses_template.name(),
template_data
            )
            input("Mail sent. Check your inbox and press Enter to continue.")

        print("Sending mail through the Amazon SES SMTP server.")
```

```
        boto3_session = boto3.Session()
        region = boto3_session.region_name
        credentials = boto3_session.get_credentials()
        port = 587
        smtp_server = f"email-smtp.{region}.amazonaws.com"
        password = calculate_key(credentials.secret_key, region)
        message = """
Subject: Hi there

This message is sent from the Amazon SES SMTP mail demo."""
        context = ssl.create_default_context()
        with smtplib.SMTP(smtp_server, port) as server:
            server.starttls(context=context)
            server.login(credentials.access_key, password)
            server.sendmail(email, email, message)
        print("Mail sent. Check your inbox!")

    if ses_template.template is not None:
        print("Deleting demo template.")
        ses_template.delete_template()
    if verified:
        answer = input(f"Do you want to remove {email} from Amazon SES (y/n)? ")
        if answer.lower() == "y":
            ses_identity.delete_identity(email)
    print("Thanks for watching!")
    print("-" * 88)
```

Erstellen von Funktionen zum Umschließen von Amazon-SES-Identitätsvorgängen.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def verify_domain_identity(self, domain_name):
```

```
        """
        Starts verification of a domain identity. To complete verification, you
 must
        create a TXT record with a specific format through your DNS provider.

        For more information, see *Verifying a domain with Amazon SES* in the
        Amazon SES documentation:
            https://docs.aws.amazon.com/ses/latest/DeveloperGuide/verify-domain-
procedure.html

        :param domain_name: The name of the domain to verify.
        :return: The token to include in the TXT record with your DNS provider.
        """
        try:
            response = self.ses_client.verify_domain_identity(Domain=domain_name)
            token = response["VerificationToken"]
            logger.info("Got domain verification token for %s.", domain_name)
        except ClientError:
            logger.exception("Couldn't verify domain %s.", domain_name)
            raise
        else:
            return token


    def verify_email_identity(self, email_address):
        """
        Starts verification of an email identity. This function causes an email
        to be sent to the specified email address from Amazon SES. To complete
        verification, follow the instructions in the email.

        :param email_address: The email address to verify.
        """
        try:
            self.ses_client.verify_email_identity(EmailAddress=email_address)
            logger.info("Started verification of %s.", email_address)
        except ClientError:
            logger.exception("Couldn't start verification of %s.", email_address)
            raise


    def wait_until_identity_exists(self, identity):
        """
        Waits until an identity exists. The waiter polls Amazon SES until the
```

```
        identity has been successfully verified or until it exceeds its maximum
time.

        :param identity: The identity to wait for.
        """
        try:
            waiter = self.ses_client.get_waiter("identity_exists")
            logger.info("Waiting until %s exists.", identity)
            waiter.wait(Identities=[identity])
        except WaiterError:
            logger.error("Waiting for identity %s failed or timed out.",
identity)
            raise


    def get_identity_status(self, identity):
        """
        Gets the status of an identity. This can be used to discover whether
        an identity has been successfully verified.

        :param identity: The identity to query.
        :return: The status of the identity.
        """
        try:
            response = self.ses_client.get_identity_verification_attributes(
                Identities=[identity]
            )
            status = response["VerificationAttributes"].get(
                identity, {"VerificationStatus": "NotFound"}
            )["VerificationStatus"]
            logger.info("Got status of %s for %s.", status, identity)
        except ClientError:
            logger.exception("Couldn't get status for %s.", identity)
            raise
        else:
            return status


    def delete_identity(self, identity):
        """
        Deletes an identity.

        :param identity: The identity to remove.
        """
```

```
        try:
            self.ses_client.delete_identity(Identity=identity)
            logger.info("Deleted identity %s.", identity)
        except ClientError:
            logger.exception("Couldn't delete identity %s.", identity)
            raise


    def list_identities(self, identity_type, max_items):
        """
        Gets the identities of the specified type for the current account.

        :param identity_type: The type of identity to retrieve, such as
 EmailAddress.
        :param max_items: The maximum number of identities to retrieve.
        :return: The list of retrieved identities.
        """
        try:
            response = self.ses_client.list_identities(
                IdentityType=identity_type, MaxItems=max_items
            )
            identities = response["Identities"]
            logger.info("Got %s identities for the current account.",
 len(identities))
        except ClientError:
            logger.exception("Couldn't list identities for the current account.")
            raise
        else:
            return identities
```

Erstellen von Funktionen zum Umschließen von Amazon-SES-Vorlagenvorgängen.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
```

```
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def create_template(self, name, subject, text, html):
        """
        Creates an email template.

        :param name: The name of the template.
        :param subject: The subject of the email.
        :param text: The plain text version of the email.
        :param html: The HTML version of the email.
        """
        try:
            template = {
                "TemplateName": name,
                "SubjectPart": subject,
                "TextPart": text,
                "HtmlPart": html,
            }
            self.ses_client.create_template(Template=template)
            logger.info("Created template %s.", name)
            self.template = template
            self._extract_tags(subject, text, html)
        except ClientError:
            logger.exception("Couldn't create template %s.", name)
            raise


    def delete_template(self):
        """
        Deletes an email template.
```

```
        """
        try:

self.ses_client.delete_template(TemplateName=self.template["TemplateName"])
            logger.info("Deleted template %s.", self.template["TemplateName"])
            self.template = None
            self.template_tags = None
        except ClientError:
            logger.exception(
                "Couldn't delete template %s.", self.template["TemplateName"]
            )
            raise


    def get_template(self, name):
        """
        Gets a previously created email template.

        :param name: The name of the template to retrieve.
        :return: The retrieved email template.
        """
        try:
            response = self.ses_client.get_template(TemplateName=name)
            self.template = response["Template"]
            logger.info("Got template %s.", name)
            self._extract_tags(
                self.template["SubjectPart"],
                self.template["TextPart"],
                self.template["HtmlPart"],
            )
        except ClientError:
            logger.exception("Couldn't get template %s.", name)
            raise
        else:
            return self.template


    def list_templates(self):
        """
        Gets a list of all email templates for the current account.

        :return: The list of retrieved email templates.
        """
        try:
```

```
            response = self.ses_client.list_templates()
            templates = response["TemplatesMetadata"]
            logger.info("Got %s templates.", len(templates))
        except ClientError:
            logger.exception("Couldn't get templates.")
            raise
        else:
            return templates


    def update_template(self, name, subject, text, html):
        """
        Updates a previously created email template.

        :param name: The name of the template.
        :param subject: The subject of the email.
        :param text: The plain text version of the email.
        :param html: The HTML version of the email.
        """
        try:
            template = {
                "TemplateName": name,
                "SubjectPart": subject,
                "TextPart": text,
                "HtmlPart": html,
            }
            self.ses_client.update_template(Template=template)
            logger.info("Updated template %s.", name)
            self.template = template
            self._extract_tags(subject, text, html)
        except ClientError:
            logger.exception("Couldn't update template %s.", name)
            raise
```

Erstellen von Funktionen zum Umschließen von Amazon-SES-E-Mail-Vorgängen.

```
class SesDestination:
    """Contains data about an email destination."""

    def __init__(self, tos, ccs=None, bccs=None):
```

```
        """
        :param tos: The list of recipients on the 'To:' line.
        :param ccs: The list of recipients on the 'CC:' line.
        :param bccs: The list of recipients on the 'BCC:' line.
        """
        self.tos = tos
        self.ccs = ccs
        self.bccs = bccs

    def to_service_format(self):
        """
        :return: The destination data in the format expected by Amazon SES.
        """
        svc_format = {"ToAddresses": self.tos}
        if self.ccs is not None:
            svc_format["CcAddresses"] = self.ccs
        if self.bccs is not None:
            svc_format["BccAddresses"] = self.bccs
        return svc_format



class SesMailSender:
    """Encapsulates functions to send emails with Amazon SES."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def send_email(self, source, destination, subject, text, html,
 reply_tos=None):
        """
        Sends an email.

        Note: If your account is in the Amazon SES  sandbox, the source and
        destination email accounts must both be verified.

        :param source: The source email account.
        :param destination: The destination email account.
        :param subject: The subject of the email.
        :param text: The plain text version of the body of the email.
```

```
        :param html: The HTML version of the body of the email.
        :param reply_tos: Email accounts that will receive a reply if the
recipient
                          replies to the message.
        :return: The ID of the message, assigned by Amazon SES.
        """
        send_args = {
            "Source": source,
            "Destination": destination.to_service_format(),
            "Message": {
                "Subject": {"Data": subject},
                "Body": {"Text": {"Data": text}, "Html": {"Data": html}},
            },
        }
        if reply_tos is not None:
            send_args["ReplyToAddresses"] = reply_tos
        try:
            response = self.ses_client.send_email(**send_args)
            message_id = response["MessageId"]
            logger.info(
                "Sent mail %s from %s to %s.", message_id, source,
destination.tos
            )
        except ClientError:
            logger.exception(
                "Couldn't send mail from %s to %s.", source, destination.tos
            )
            raise
        else:
            return message_id


    def send_templated_email(
        self, source, destination, template_name, template_data, reply_tos=None
    ):
        """
        Sends an email based on a template. A template contains replaceable tags
        each enclosed in two curly braces, such as {{name}}. The template data
passed
        in this function contains key-value pairs that define the values to
insert
        in place of the template tags.

        Note: If your account is in the Amazon SES  sandbox, the source and
```

```
        destination email accounts must both be verified.

        :param source: The source email account.
        :param destination: The destination email account.
        :param template_name: The name of a previously created template.
        :param template_data: JSON-formatted key-value pairs of replacement
values
                              that are inserted in the template before it is
sent.
        :return: The ID of the message, assigned by Amazon SES.
        """
        send_args = {
            "Source": source,
            "Destination": destination.to_service_format(),
            "Template": template_name,
            "TemplateData": json.dumps(template_data),
        }
        if reply_tos is not None:
            send_args["ReplyToAddresses"] = reply_tos
        try:
            response = self.ses_client.send_templated_email(**send_args)
            message_id = response["MessageId"]
            logger.info(
                "Sent templated mail %s from %s to %s.",
                message_id,
                source,
                destination.tos,
            )
        except ClientError:
            logger.exception(
                "Couldn't send templated mail from %s to %s.", source,
destination.tos
            )
            raise
        else:
            return message_id
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS SDK für Python (Boto3).
  - CreateTemplate

- DeleteIdentity
- DeleteTemplate
- GetIdentityVerificationAttributes
- GetTemplate
- ListIdentities
- ListTemplates
- SendEmail
- SendTemplatedEmail
- UpdateTemplate
- VerifyDomainIdentity
- VerifyEmailIdentity

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele für Amazon SES API v2 mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Amazon SES API v2 mit einem AWS Software Development Kit (SDK) verwendet wird.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Service-Funktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien anzeigen.

Szenarien sind Codebeispiele, die Ihnen zeigen, wie Sie bestimmte Aufgaben ausführen, indem Sie mehrere Funktionen innerhalb eines Service aufrufen oder mit anderen AWS-Services kombinieren.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Amazon SES API v2

- Grundlegende Beispiele für die Verwendung von Amazon SES API v2 AWS SDKs
  - Aktionen für Amazon SES API v2 mit AWS SDKs

    - Verwenden Sie es CreateContact mit einem AWS SDK
    - CreateContactListMit einem AWS SDK verwenden
    - CreateEmailIdentityMit einem AWS SDK verwenden
    - CreateEmailTemplateMit einem AWS SDK verwenden
    - DeleteContactListMit einem AWS SDK verwenden
    - DeleteEmailIdentityMit einem AWS SDK verwenden
    - DeleteEmailTemplateMit einem AWS SDK verwenden
    - GetEmailIdentityMit einem AWS SDK verwenden
    - ListContactListsMit einem AWS SDK verwenden
    - ListContactsMit einem AWS SDK verwenden
    - SendEmailMit einem AWS SDK verwenden
- Szenarien für die Verwendung von Amazon SES API v2 AWS SDKs
    - Ein vollständiges Amazon SES API v2-Newsletter-Szenario mit einem AWS SDK

Grundlegende Beispiele für die Verwendung von Amazon SES API v2 AWS SDKs

Die folgenden Codebeispiele zeigen, wie Sie die Grundlagen der Amazon Simple Email Service API v2 mit verwenden können AWS SDKs.

Beispiele

- Aktionen für Amazon SES API v2 mit AWS SDKs
    - Verwenden Sie es CreateContact mit einem AWS SDK
    - CreateContactListMit einem AWS SDK verwenden
    - CreateEmailIdentityMit einem AWS SDK verwenden
    - CreateEmailTemplateMit einem AWS SDK verwenden
    - DeleteContactListMit einem AWS SDK verwenden
    - DeleteEmailIdentityMit einem AWS SDK verwenden
    - DeleteEmailTemplateMit einem AWS SDK verwenden
    - GetEmailIdentityMit einem AWS SDK verwenden
    - ListContactListsMit einem AWS SDK verwenden

- ListContactsMit einem AWS SDK verwenden
- SendEmailMit einem AWS SDK verwenden

Aktionen für Amazon SES API v2 mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie einzelne Amazon SES API v2-Aktionen mit ausgeführt AWS SDKs werden. Jedes Beispiel enthält einen Link zu GitHub, über den Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Diese Auszüge rufen die API „Amazon-SES-API v2“ auf und sind Codeauszüge aus größeren Programmen, die im Kontext ausgeführt werden müssen. Sie können Aktionen im Kontext unter Szenarien für die Verwendung von Amazon SES API v2 AWS SDKs anzeigen.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der API-Referenz zu Amazon Simple Email Service API v2.

Beispiele

- Verwenden Sie es CreateContact mit einem AWS SDK
- CreateContactListMit einem AWS SDK verwenden
- CreateEmailIdentityMit einem AWS SDK verwenden
- CreateEmailTemplateMit einem AWS SDK verwenden
- DeleteContactListMit einem AWS SDK verwenden
- DeleteEmailIdentityMit einem AWS SDK verwenden
- DeleteEmailTemplateMit einem AWS SDK verwenden
- GetEmailIdentityMit einem AWS SDK verwenden
- ListContactListsMit einem AWS SDK verwenden
- ListContactsMit einem AWS SDK verwenden
- SendEmailMit einem AWS SDK verwenden

Verwenden Sie es **`CreateContact`** mit einem AWS SDK

Die folgenden Code-Beispiele zeigen, wie `CreateContact` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Newsletter-Szenario

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Creates a contact and adds it to the specified contact list.
    /// </summary>
    /// <param name="emailAddress">The email address of the contact.</param>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>The response from the CreateContact operation.</returns>
    public async Task<bool> CreateContactAsync(string emailAddress, string
contactListName)
    {
        var request = new CreateContactRequest
        {
            EmailAddress = emailAddress,
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.CreateContactAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Contact with email address {emailAddress} already
exists in the contact list {contactListName}.");
            Console.WriteLine(ex.Message);
            return true;
        }
        catch (NotFoundException ex)
        {
```

```
            Console.WriteLine($"The contact list {contactListName} does not
exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the contact:
{ex.Message}");
        }
        return false;
    }
```

- Einzelheiten zur API finden Sie CreateContactin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    try {
      // Create a new contact with the provided email address in the
      CreateContactRequest contactRequest = CreateContactRequest.builder()
          .contactListName(CONTACT_LIST_NAME)
          .emailAddress(emailAddress)
          .build();

      sesClient.createContact(contactRequest);
      contacts.add(emailAddress);

      System.out.println("Contact created: " + emailAddress);
```

```
        // Send a welcome email to the new contact
        String welcomeHtml = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.html"));
        String welcomeText = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.txt"));

        SendEmailRequest welcomeEmailRequest = SendEmailRequest.builder()
            .fromEmailAddress(this.verifiedEmail)
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .simple(
                    Message.builder()
                        .subject(Content.builder().data("Welcome to the Weekly
 Coupons Newsletter").build())
                        .body(Body.builder()
                            .text(Content.builder().data(welcomeText).build())
                            .html(Content.builder().data(welcomeHtml).build())
                            .build())
                        .build())
                .build())
            .build();
        SendEmailResponse welcomeEmailResponse =
 sesClient.sendEmail(welcomeEmailRequest);
        System.out.println("Welcome email sent: " +
 welcomeEmailResponse.messageId());
      } catch (AlreadyExistsException e) {
        // If the contact already exists, skip this step for that contact and
 proceed
        // with the next contact
        System.out.println("Contact already exists, skipping creation...");
      } catch (Exception e) {
        System.err.println("Error occurred while processing email address " +
 emailAddress + ": " + e.getMessage());
        throw e;
      }
    }
```

- Einzelheiten zur API finden Sie CreateContactin der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


            try:
                # Create a new contact
                self.ses_client.create_contact(
                    ContactListName=CONTACT_LIST_NAME, EmailAddress=email
```

```
                )
                print(f"Contact with email '{email}' created successfully.")

                # Send the welcome email
                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")
                if self.sleep:
                    # 1 email per second in sandbox mode, remove in production.
                    sleep(1.1)
            except ClientError as e:
                # If the contact already exists, skip and proceed
                if e.response["Error"]["Code"] == "AlreadyExistsException":
                    print(f"Contact with email '{email}' already exists.
Skipping...")
                else:
                    raise e
```

- Einzelheiten zur API finden Sie CreateContactin AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn add_contact(client: &Client, list: &str, email: &str) -> Result<(),
 Error> {
    client
        .create_contact()
        .contact_list_name(list)
        .email_address(email)
        .send()
        .await?;

    println!("Created contact");

    Ok(())
}
```

- Einzelheiten zur API finden Sie CreateContactin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    TRY.
        lo_se2->createcontact(
          iv_contactlistname = iv_contact_list_name
```

```
          iv_emailaddress = iv_email_address ).
        MESSAGE 'Contact created successfully.' TYPE 'I'.
      CATCH /aws1/cx_se2alreadyexistsex.
        MESSAGE 'Contact already exists.' TYPE 'I'.
      CATCH /aws1/cx_se2badrequestex.
        MESSAGE 'Bad request.' TYPE 'E'.
      CATCH /aws1/cx_se2notfoundexception.
        MESSAGE 'Contact list not found.' TYPE 'E'.
    ENDTRY.
```

- Einzelheiten zur API finden Sie CreateContactin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`CreateContactList`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `CreateContactList` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Newsletter-Szenario

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Creates a contact list with the specified name.
    /// </summary>
```

```
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateContactListAsync(string contactListName)
    {
        var request = new CreateContactListRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.CreateContactListAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Contact list with name {contactListName} already
exists.");
            Console.WriteLine(ex.Message);
            return true;
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for contact lists has been exceeded.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the contact
list: {ex.Message}");
        }
        return false;
    }
```

- Einzelheiten zur API finden Sie CreateContactListin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    try {
      // 2. Create a contact list
      String contactListName = CONTACT_LIST_NAME;
      CreateContactListRequest createContactListRequest =
 CreateContactListRequest.builder()
          .contactListName(contactListName)
          .build();
      sesClient.createContactList(createContactListRequest);
      System.out.println("Contact list created: " + contactListName);
    } catch (AlreadyExistsException e) {
      System.out.println("Contact list already exists, skipping creation: weekly-
coupons-newsletter");
    } catch (LimitExceededException e) {
      System.err.println("Limit for contact lists has been exceeded.");
      throw e;
    } catch (SesV2Exception e) {
      System.err.println("Error creating contact list: " + e.getMessage());
      throw e;
    }
```

- Einzelheiten zur API finden Sie CreateContactListin der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.create_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' created successfully.")
```

```
        except ClientError as e:
            # If the contact list already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Contact list '{CONTACT_LIST_NAME}' already exists.")
            else:
                raise e
```

- Einzelheiten zur API finden Sie CreateContactListin AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn make_list(client: &Client, contact_list: &str) -> Result<(), Error> {
    client
        .create_contact_list()
        .contact_list_name(contact_list)
        .send()
        .await?;

    println!("Created contact list.");

    Ok(())
}
```

- Einzelheiten zur API finden Sie CreateContactListin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_se2->createcontactlist(
      iv_contactlistname = iv_contact_list_name ).
    MESSAGE 'Contact list created successfully.' TYPE 'I'.
  CATCH /aws1/cx_se2alreadyexistsex.
    MESSAGE 'Contact list already exists.' TYPE 'I'.
  CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
    MESSAGE 'Bad request - contact list limit may be reached.' TYPE 'I'.
    " Re-raise the exception so the caller can handle it
    RAISE EXCEPTION lo_bad_request.
  CATCH /aws1/cx_se2limitexceededex INTO DATA(lo_limit_exceeded).
    MESSAGE 'Limit exceeded - contact list limit reached.' TYPE 'I'.
    " Re-raise the exception so the caller can handle it
    RAISE EXCEPTION lo_limit_exceeded.
ENDTRY.
```

- Einzelheiten zur API finden Sie CreateContactListin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`CreateEmailIdentity`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `CreateEmailIdentity` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Newsletter-Szenario

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   /// <summary>
   /// Creates an email identity (email address or domain) and starts the
verification process.
   /// </summary>
   /// <param name="emailIdentity">The email address or domain to create and
verify.</param>
   /// <returns>The response from the CreateEmailIdentity operation.</returns>
   public async Task<CreateEmailIdentityResponse>
CreateEmailIdentityAsync(string emailIdentity)
   {
       var request = new CreateEmailIdentityRequest
       {
           EmailIdentity = emailIdentity
       };

       try
       {
           var response = await _sesClient.CreateEmailIdentityAsync(request);
           return response;
       }
       catch (AlreadyExistsException ex)
       {
           Console.WriteLine($"Email identity {emailIdentity} already exists.");
           Console.WriteLine(ex.Message);
           throw;
       }
       catch (ConcurrentModificationException ex)
       {
           Console.WriteLine($"The email identity {emailIdentity} is being
modified by another operation or thread.");
```

```
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for email identities has been
exceeded.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} does not
exist.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the email
identity: {ex.Message}");
            throw;
        }
    }
```

- Einzelheiten zur API finden Sie CreateEmailIdentityin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   try {
     CreateEmailIdentityRequest createEmailIdentityRequest =
CreateEmailIdentityRequest.builder()
         .emailIdentity(verifiedEmail)
         .build();
     sesClient.createEmailIdentity(createEmailIdentityRequest);
     System.out.println("Email identity created: " + verifiedEmail);
   } catch (AlreadyExistsException e) {
     System.out.println("Email identity already exists, skipping creation: " +
verifiedEmail);
   } catch (NotFoundException e) {
     System.err.println("The provided email address is not verified: " +
verifiedEmail);
     throw e;
   } catch (LimitExceededException e) {
     System.err
         .println("You have reached the limit for email identities. Please
remove some identities and try again.");
     throw e;
   } catch (SesV2Exception e) {
     System.err.println("Error creating email identity: " + e.getMessage());
     throw e;
   }
```

- Einzelheiten zur API finden Sie CreateEmailIdentityin der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.create_email_identity(EmailIdentity=self.verified_email)
```

```
            print(f"Email identity '{self.verified_email}' created
successfully.")
        except ClientError as e:
            # If the email identity already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email identity '{self.verified_email}' already exists.")
            else:
                raise e
```

- Einzelheiten zur API finden Sie CreateEmailIdentityin AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
        match self
            .client
            .create_email_identity()
            .email_identity(self.verified_email.clone())
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email identity created
successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateEmailIdentityError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Email identity already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating email identity: {}", e)),
            },
```

```
        }
```

- Einzelheiten zur API finden Sie CreateEmailIdentityin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_se2->createemailidentity(
      iv_emailidentity = iv_email_identity ).
    MESSAGE 'Email identity created successfully.' TYPE 'I'.
  CATCH /aws1/cx_se2alreadyexistsex.
    MESSAGE 'Email identity already exists.' TYPE 'I'.
  CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
    MESSAGE lo_bad_request TYPE 'I' DISPLAY LIKE 'E'.
  CATCH /aws1/cx_se2limitexceededex INTO DATA(lo_limit_exceeded).
    MESSAGE lo_limit_exceeded TYPE 'I' DISPLAY LIKE 'E'.
ENDTRY.
```

- Einzelheiten zur API finden Sie CreateEmailIdentityin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`CreateEmailTemplate`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `CreateEmailTemplate` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Newsletter-Szenario

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Creates an email template with the specified content.
    /// </summary>
    /// <param name="templateName">The name of the email template.</param>
    /// <param name="subject">The subject of the email template.</param>
    /// <param name="htmlContent">The HTML content of the email template.</param>
    /// <param name="textContent">The text content of the email template.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateEmailTemplateAsync(string templateName, string
subject, string htmlContent, string textContent)
    {
        var request = new CreateEmailTemplateRequest
        {
            TemplateName = templateName,
            TemplateContent = new EmailTemplateContent
            {
                Subject = subject,
                Html = htmlContent,
                Text = textContent
            }
        };

        try
        {
            var response = await _sesClient.CreateEmailTemplateAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
```

```
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Email template with name {templateName} already
exists.");
            Console.WriteLine(ex.Message);
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for email templates has been
exceeded.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the email
template: {ex.Message}");
        }

        return false;
    }
```

- Einzelheiten zur API finden Sie CreateEmailTemplatein der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    try {
      // Create an email template named "weekly-coupons"
      String newsletterHtml = loadFile("resources/coupon_newsletter/coupon-
newsletter.html");
      String newsletterText = loadFile("resources/coupon_newsletter/coupon-
newsletter.txt");

      CreateEmailTemplateRequest templateRequest =
 CreateEmailTemplateRequest.builder()
          .templateName(TEMPLATE_NAME)
          .templateContent(EmailTemplateContent.builder()
              .subject("Weekly Coupons Newsletter")
              .html(newsletterHtml)
              .text(newsletterText)
              .build())
          .build();

      sesClient.createEmailTemplate(templateRequest);

      System.out.println("Email template created: " + TEMPLATE_NAME);
    } catch (AlreadyExistsException e) {
      // If the template already exists, skip this step and proceed with the next
      // operation
      System.out.println("Email template already exists, skipping creation...");
    } catch (LimitExceededException e) {
      // If the limit for email templates is exceeded, fail the workflow and
 inform
      // the user
      System.err.println("You have reached the limit for email templates. Please
 remove some templates and try again.");
      throw e;
    } catch (Exception e) {
      System.err.println("Error occurred while creating email template: " +
e.getMessage());
      throw e;
    }
```

- Einzelheiten zur API finden Sie CreateEmailTemplatein der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:
            template_content = {
                "Subject": "Weekly Coupons Newsletter",
                "Html": load_file_content("coupon-newsletter.html"),
```

```
                "Text": load_file_content("coupon-newsletter.txt"),
            }
            self.ses_client.create_email_template(
                TemplateName=TEMPLATE_NAME, TemplateContent=template_content
            )
            print(f"Email template '{TEMPLATE_NAME}' created successfully.")
        except ClientError as e:
            # If the template already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email template '{TEMPLATE_NAME}' already exists.")
            else:
                raise e
```

- Einzelheiten zur API finden Sie CreateEmailTemplatein AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
        let template_html =
            std::fs::read_to_string("../resources/newsletter/coupon-
newsletter.html")
                .unwrap_or_else(|_| "Missing coupon-
newsletter.html".to_string());
        let template_text =
            std::fs::read_to_string("../resources/newsletter/coupon-
newsletter.txt")
                .unwrap_or_else(|_| "Missing coupon-newsletter.txt".to_string());

        // Create the email template
        let template_content = EmailTemplateContent::builder()
            .subject("Weekly Coupons Newsletter")
            .html(template_html)
```

```
            .text(template_text)
            .build();

        match self
            .client
            .create_email_template()
            .template_name(TEMPLATE_NAME)
            .template_content(template_content)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email template created
successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateEmailTemplateError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Email template already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating email template: {}", e)),
            },
        }
```

- Einzelheiten zur API finden Sie CreateEmailTemplatein der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    TRY.
        DATA(lo_template_content) = NEW /aws1/cl_se2emailtmplcontent(
          iv_subject = iv_subject
```

```
          iv_html = iv_html
          iv_text = iv_text ).

        lo_se2->createemailtemplate(
          iv_templatename = iv_template_name
          io_templatecontent = lo_template_content ).
        MESSAGE 'Email template created successfully.' TYPE 'I'.
      CATCH /aws1/cx_se2alreadyexistsex.
        MESSAGE 'Email template already exists.' TYPE 'I'.
      CATCH /aws1/cx_se2badrequestex.
        MESSAGE 'Bad request.' TYPE 'E'.
      CATCH /aws1/cx_se2limitexceededex.
        MESSAGE 'Limit exceeded.' TYPE 'E'.
    ENDTRY.
```

- Einzelheiten zur API finden Sie CreateEmailTemplatein der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`DeleteContactList`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `DeleteContactList` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Newsletter-Szenario

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Deletes a contact list and all contacts within it.
    /// </summary>
    /// <param name="contactListName">The name of the contact list to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteContactListAsync(string contactListName)
    {
        var request = new DeleteContactListRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.DeleteContactListAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The contact list {contactListName} is being
 modified by another operation or thread.");
            Console.WriteLine(ex.Message);
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while deleting the contact
 list: {ex.Message}");
        }

        return false;
```

```
    }
```

- Einzelheiten zur API finden Sie DeleteContactListin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   try {
     // Delete the contact list
     DeleteContactListRequest deleteContactListRequest =
DeleteContactListRequest.builder()
         .contactListName(CONTACT_LIST_NAME)
         .build();

     sesClient.deleteContactList(deleteContactListRequest);

     System.out.println("Contact list deleted: " + CONTACT_LIST_NAME);
   } catch (NotFoundException e) {
     // If the contact list does not exist, log the error and proceed
     System.out.println("Contact list not found. Skipping deletion...");
   } catch (Exception e) {
     System.err.println("Error occurred while deleting the contact list: " +
e.getMessage());
     e.printStackTrace();
   }
```

- Einzelheiten zur API finden Sie DeleteContactListin der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.delete_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' deleted successfully.")
```

```
        except ClientError as e:
            # If the contact list doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
            else:
                print(e)
```

- Einzelheiten zur API finden Sie DeleteContactListin AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
        match self
            .client
            .delete_contact_list()
            .contact_list_name(CONTACT_LIST_NAME)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Contact list deleted
successfully.")?,
            Err(e) => return Err(anyhow!("Error deleting contact list: {e}")),
        }
```

- Einzelheiten zur API finden Sie DeleteContactListin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_se2->deletecontactlist(
      iv_contactlistname = iv_contact_list_name ).
    MESSAGE 'Contact list deleted successfully.' TYPE 'I'.
  CATCH /aws1/cx_se2notfoundexception.
    MESSAGE 'Contact list not found.' TYPE 'I'.
  CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
    MESSAGE 'Bad request.' TYPE 'I'.
    RAISE EXCEPTION lo_bad_request.
ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteContactListin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`DeleteEmailIdentity`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `DeleteEmailIdentity` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Newsletter-Szenario

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Deletes an email identity (email address or domain).
    /// </summary>
    /// <param name="emailIdentity">The email address or domain to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailIdentityAsync(string emailIdentity)
    {
        var request = new DeleteEmailIdentityRequest
        {
            EmailIdentity = emailIdentity
        };

        try
        {
            var response = await _sesClient.DeleteEmailIdentityAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} is being
 modified by another operation or thread.");
            Console.WriteLine(ex.Message);
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
```

```
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while deleting the email
identity: {ex.Message}");
        }

        return false;
    }
```

- Einzelheiten zur API finden Sie DeleteEmailIdentityin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
     try {
       // Delete the email identity
       DeleteEmailIdentityRequest deleteIdentityRequest =
DeleteEmailIdentityRequest.builder()
            .emailIdentity(this.verifiedEmail)
            .build();

       sesClient.deleteEmailIdentity(deleteIdentityRequest);

       System.out.println("Email identity deleted: " + this.verifiedEmail);
     } catch (NotFoundException e) {
       // If the email identity does not exist, log the error and proceed
       System.out.println("Email identity not found. Skipping deletion...");
     } catch (Exception e) {
       System.err.println("Error occurred while deleting the email identity: " +
e.getMessage());
```

```
            e.printStackTrace();
        }
    } else {
        System.out.println("Skipping email identity deletion.");
    }
```

- Einzelheiten zur API finden Sie DeleteEmailIdentityin der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
```

```
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


            try:

self.ses_client.delete_email_identity(EmailIdentity=self.verified_email)
                print(f"Email identity '{self.verified_email}' deleted
successfully.")
            except ClientError as e:
                # If the email identity doesn't exist, skip and proceed
                if e.response["Error"]["Code"] == "NotFoundException":
                    print(f"Email identity '{self.verified_email}' does not
exist.")
                else:
                    print(e)
```

- Einzelheiten zur API finden Sie DeleteEmailIdentityin AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
            match self
                .client
                .delete_email_identity()
                .email_identity(self.verified_email.clone())
                .send()
                .await
            {
```

```
                Ok(_) => writeln!(self.stdout, "Email identity deleted
successfully.")?,
                Err(e) => {
                    return Err(anyhow!("Error deleting email identity: {}", e));
                }
            }
```

- Einzelheiten zur API finden Sie DeleteEmailIdentityin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_se2->deleteemailidentity(
      iv_emailidentity = iv_email_identity ).
    MESSAGE 'Email identity deleted successfully.' TYPE 'I'.
  CATCH /aws1/cx_se2notfoundexception.
    MESSAGE 'Email identity not found.' TYPE 'I'.
  CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
    MESSAGE 'Bad request.' TYPE 'I'.
    RAISE EXCEPTION lo_bad_request.
ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteEmailIdentityin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`DeleteEmailTemplate`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `DeleteEmailTemplate` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Newsletter-Szenario

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Deletes an email template.
    /// </summary>
    /// <param name="templateName">The name of the email template to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailTemplateAsync(string templateName)
    {
        var request = new DeleteEmailTemplateRequest
        {
            TemplateName = templateName
        };

        try
        {
            var response = await _sesClient.DeleteEmailTemplateAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email template {templateName} does not
 exist.");
```

```
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while deleting the email
template: {ex.Message}");
        }

        return false;
    }
```

- Einzelheiten zur API finden Sie DeleteEmailTemplatein der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    try {
      // Delete the template
      DeleteEmailTemplateRequest deleteTemplateRequest =
DeleteEmailTemplateRequest.builder()
          .templateName(TEMPLATE_NAME)
          .build();

      sesClient.deleteEmailTemplate(deleteTemplateRequest);

      System.out.println("Email template deleted: " + TEMPLATE_NAME);
```

```
    } catch (NotFoundException e) {
      // If the email template does not exist, log the error and proceed
      System.out.println("Email template not found. Skipping deletion...");
    } catch (Exception e) {
      System.err.println("Error occurred while deleting the email template: " +
 e.getMessage());
      e.printStackTrace();
    }
```

- Einzelheiten zur API finden Sie DeleteEmailTemplatein der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()
```

```
class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:
            self.ses_client.delete_email_template(TemplateName=TEMPLATE_NAME)
            print(f"Email template '{TEMPLATE_NAME}' deleted successfully.")
        except ClientError as e:
            # If the email template doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Email template '{TEMPLATE_NAME}' does not exist.")
            else:
                print(e)
```

- Einzelheiten zur API finden Sie DeleteEmailTemplatein AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
        match self
            .client
            .delete_email_template()
            .template_name(TEMPLATE_NAME)
            .send()
            .await
        {
```

```
            Ok(_) => writeln!(self.stdout, "Email template deleted
successfully.")?,
            Err(e) => {
                return Err(anyhow!("Error deleting email template: {e}"));
            }
        }
```

- Einzelheiten zur API finden Sie DeleteEmailTemplatein der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    lo_se2->deleteemailtemplate(
      iv_templatename = iv_template_name ).
    MESSAGE 'Email template deleted successfully.' TYPE 'I'.
  CATCH /aws1/cx_se2notfoundexception.
    MESSAGE 'Email template not found.' TYPE 'I'.
  CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
    MESSAGE 'Bad request.' TYPE 'I'.
    RAISE EXCEPTION lo_bad_request.
ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteEmailTemplatein der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`GetEmailIdentity`Mit einem AWS SDK verwenden

Das folgende Codebeispiel zeigt, wie es verwendet wird`GetEmailIdentity`.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Bestimmt, ob eine E-Mail-Adresse überprüft wurde.

```
async fn is_verified(client: &Client, email: &str) -> Result<(), Error> {
    let resp = client
        .get_email_identity()
        .email_identity(email)
        .send()
        .await?;

    if resp.verified_for_sending_status() {
        println!("The address is verified");
    } else {
        println!("The address is not verified");
    }

    Ok(())
}
```

- Einzelheiten zur API finden Sie GetEmailIdentityin der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`ListContactLists`Mit einem AWS SDK verwenden

Das folgende Codebeispiel zeigt, wie es verwendet wird`ListContactLists`.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn show_lists(client: &Client) -> Result<(), Error> {
    let resp = client.list_contact_lists().send().await?;

    println!("Contact lists:");

    for list in resp.contact_lists() {
        println!("  {}", list.contact_list_name().unwrap_or_default());
    }

    Ok(())
}
```

- Einzelheiten zur API finden Sie ListContactListsin der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`ListContacts`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `ListContacts` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Newsletter-Szenario

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Lists the contacts in the specified contact list.
    /// </summary>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>The list of contacts response from the ListContacts operation.</
returns>
    public async Task<List<Contact>> ListContactsAsync(string contactListName)
    {
        var request = new ListContactsRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.ListContactsAsync(request);
            return response.Contacts;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
```

```
            Console.WriteLine($"An error occurred while listing the contacts:
{ex.Message}");
        }

        return new List<Contact>();
    }
```

- Einzelheiten zur API finden Sie ListContactsin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
     ListContactsRequest contactListRequest = ListContactsRequest.builder()
         .contactListName(CONTACT_LIST_NAME)
         .build();

     List<String> contactEmails;
     try {
       ListContactsResponse contactListResponse =
sesClient.listContacts(contactListRequest);

       contactEmails = contactListResponse.contacts().stream()
           .map(Contact::emailAddress)
           .toList();
     } catch (Exception e) {
       // TODO: Remove when listContacts's GET body issue is resolved.
       contactEmails = this.contacts;
     }
```

- Einzelheiten zur API finden Sie ListContactsin der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:
            contacts_response = self.ses_client.list_contacts(
                ContactListName=CONTACT_LIST_NAME
            )
```

```
        except ClientError as e:
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
                return
            else:
                raise e
```

- Einzelheiten zur API finden Sie ListContactsin AWS SDK for Python (Boto3) API Reference.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn show_contacts(client: &Client, list: &str) -> Result<(), Error> {
    let resp = client
        .list_contacts()
        .contact_list_name(list)
        .send()
        .await?;

    println!("Contacts:");

    for contact in resp.contacts() {
        println!("  {}", contact.email_address().unwrap_or_default());
    }

    Ok(())
}
```

- Einzelheiten zur API finden Sie ListContactsin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
TRY.
    oo_result = lo_se2->listcontacts(
      iv_contactlistname = iv_contact_list_name ).
    DATA(lv_count) = lines( oo_result->get_contacts( ) ).
    MESSAGE |Retrieved { lv_count } contacts from list.| TYPE 'I'.
  CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
    MESSAGE 'Bad request.' TYPE 'I'.
    RAISE EXCEPTION lo_bad_request.
  CATCH /aws1/cx_se2notfoundexception INTO DATA(lo_not_found).
    MESSAGE 'Contact list not found.' TYPE 'I'.
    RAISE EXCEPTION lo_not_found.
ENDTRY.
```

- Einzelheiten zur API finden Sie ListContactsin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`SendEmail`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `SendEmail` verwendet wird.

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   /// <summary>
   /// Sends an email with the specified content and options.
   /// </summary>
   /// <param name="fromEmailAddress">The email address to send the email
from.</param>
   /// <param name="toEmailAddresses">The email addresses to send the email
to.</param>
   /// <param name="subject">The subject of the email.</param>
   /// <param name="htmlContent">The HTML content of the email.</param>
   /// <param name="textContent">The text content of the email.</param>
   /// <param name="templateName">The name of the email template to use
(optional).</param>
   /// <param name="templateData">The data to replace placeholders in the email
template (optional).</param>
   /// <param name="contactListName">The name of the contact list for
unsubscribe functionality (optional).</param>
   /// <returns>The MessageId response from the SendEmail operation.</returns>
   public async Task<string> SendEmailAsync(string fromEmailAddress,
List<string> toEmailAddresses, string? subject,
       string? htmlContent, string? textContent, string? templateName = null,
string? templateData = null, string? contactListName = null)
   {
       var request = new SendEmailRequest
       {
           FromEmailAddress = fromEmailAddress
       };

       if (toEmailAddresses.Any())
       {
           request.Destination = new Destination { ToAddresses =
toEmailAddresses };
       }
```

```
        if (!string.IsNullOrEmpty(templateName))
        {
            request.Content = new EmailContent()
            {
                Template = new Template
                {
                    TemplateName = templateName,
                    TemplateData = templateData
                }
            };
        }
        else
        {
            request.Content = new EmailContent
            {
                Simple = new Message
                {
                    Subject = new Content { Data = subject },
                    Body = new Body
                    {
                        Html = new Content { Data = htmlContent },
                        Text = new Content { Data = textContent }
                    }
                }
            };
        }

        if (!string.IsNullOrEmpty(contactListName))
        {
            request.ListManagementOptions = new ListManagementOptions
            {
                ContactListName = contactListName
            };
        }

        try
        {
            var response = await _sesClient.SendEmailAsync(request);
            return response.MessageId;
        }
        catch (AccountSuspendedException ex)
        {
```

```
            Console.WriteLine("The account's ability to send email has been
permanently restricted.");
            Console.WriteLine(ex.Message);
        }
        catch (MailFromDomainNotVerifiedException ex)
        {
            Console.WriteLine("The sending domain is not verified.");
            Console.WriteLine(ex.Message);
        }
        catch (MessageRejectedException ex)
        {
            Console.WriteLine("The message content is invalid.");
            Console.WriteLine(ex.Message);
        }
        catch (SendingPausedException ex)
        {
            Console.WriteLine("The account's ability to send email is currently
paused.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while sending the email:
{ex.Message}");
        }

        return string.Empty;
    }
```

- Einzelheiten zur API finden Sie SendEmailin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Sendet eine Nachricht.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sesv2.model.Body;
import software.amazon.awssdk.services.sesv2.model.Content;
import software.amazon.awssdk.services.sesv2.model.Destination;
import software.amazon.awssdk.services.sesv2.model.EmailContent;
import software.amazon.awssdk.services.sesv2.model.Message;
import software.amazon.awssdk.services.sesv2.model.SendEmailRequest;
import software.amazon.awssdk.services.sesv2.model.SesV2Exception;
import software.amazon.awssdk.services.sesv2.SesV2Client;

/**
 * Before running this AWS SDK for Java (v2) example, set up your development
 * environment, including your credentials.
 * <p>
 * For more information, see the following documentation topic:
 * <p>
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class SendEmail {
    public static void main(String[] args) {
        final String usage = """

                             Usage:
                                 <sender> <recipient> <subject>\s

                             Where:
                                 sender - An email address that represents the
 sender.\s
```

```
                                recipient - An email address that represents the
 recipient.\s
                                subject - The subject line.\s
                            """;

        if (args.length != 3) {
            System.out.println(usage);
            System.exit(1);
        }

        String sender = args[0];
        String recipient = args[1];
        String subject = args[2];

        Region region = Region.US_EAST_1;
        SesV2Client sesv2Client = SesV2Client.builder()
                .region(region)
                .build();

        // The HTML body of the email.
        String bodyHTML = "<html>" + "<head></head>" + "<body>" + "<h1>Hello!</
h1>"
                + "<p> See the list of customers.</p>" + "</body>" + "</html>";

        send(sesv2Client, sender, recipient, subject, bodyHTML);
    }

    public static void send(SesV2Client client,
                            String sender,
                            String recipient,
                            String subject,
                            String bodyHTML) {

        Destination destination = Destination.builder()
                .toAddresses(recipient)
                .build();

        Content content = Content.builder()
                .data(bodyHTML)
                .build();

        Content sub = Content.builder()
                .data(subject)
                .build();
```

```
        Body body = Body.builder()
                .html(content)
                .build();

        Message msg = Message.builder()
                .subject(sub)
                .body(body)
                .build();

        EmailContent emailContent = EmailContent.builder()
                .simple(msg)
                .build();

        SendEmailRequest emailRequest = SendEmailRequest.builder()
                .destination(destination)
                .content(emailContent)
                .fromEmailAddress(sender)
                .build();

        try {
            System.out.println("Attempting to send an email through Amazon SES "
                    + "using the AWS SDK for Java...");
            client.sendEmail(emailRequest);
            System.out.println("email was sent");

        } catch (SesV2Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

Sendet eine Nachricht unter Verwendung einer Vorlage.

```
      String coupons = Files.readString(Paths.get("resources/coupon_newsletter/
sample_coupons.json"));
      for (String emailAddress : contactEmails) {
        SendEmailRequest newsletterRequest = SendEmailRequest.builder()
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .template(Template.builder()
```

```
                    .templateName(TEMPLATE_NAME)
                    .templateData(coupons)
                    .build())
                .build())
            .fromEmailAddress(this.verifiedEmail)
            .listManagementOptions(ListManagementOptions.builder()
                .contactListName(CONTACT_LIST_NAME)
                .build())
            .build();
        SendEmailResponse newsletterResponse =
 sesClient.sendEmail(newsletterRequest);
        System.out.println("Newsletter sent to " + emailAddress + ": " +
 newsletterResponse.messageId());
     }
```

Sendet eine Nachricht mit Header-Informationen.

```
public class SendwithHeader {

    public static void main(String[] args) {
        final String usage = """

            Usage:
                <sender> <recipient> <subject>\s

            Where:
                sender - An email address that represents the sender.\s
                recipient - An email address that represents the recipient.\s
                subject - The subject line.\s
            """;

        if (args.length != 3) {
            System.out.println(usage);
            System.exit(1);
        }

        String sender = args[0];
        String recipient = args[1];
        String subject = args[2];
        Region region = Region.US_EAST_1;
        SesV2Client sesv2Client = SesV2Client.builder()
                .region(region)
```

```
                .build();

        String bodyHTML = """
                <html>
                    <head></head>
                    <body>
                        <h1>Hello!</h1>
                        <p>See the list of customers.</p>
                    </body>
                </html>
                """;

        sendWithHeader(sesv2Client, sender, recipient, subject, bodyHTML);
        sesv2Client.close();
    }

    /**
     * Sends an email using the AWS SES V2 client.
     *
     * @param sesv2Client the SES V2 client to use for sending the email
     * @param sender the email address of the sender
     * @param recipient the email address of the recipient
     * @param subject the subject of the email
     * @param bodyHTML the HTML content of the email body
     */
    public static void sendWithHeader(SesV2Client sesv2Client,
                                      String sender,
                                      String recipient,
                                      String subject,
                                      String bodyHTML) {
        EmailContent emailContent = EmailContent.builder()
                .simple(Message.builder()
                        .body(b -> b.html(c ->
 c.charset(UTF_8.name()).data(bodyHTML))
                                .text(c ->
 c.charset(UTF_8.name()).data(bodyHTML)))
                        .subject(c -> c.charset(UTF_8.name()).data(subject))
                        .headers(List.of(
                                MessageHeader.builder()
                                        .name("List-Unsubscribe")
                                        .value("<https://nutrition.co/?
address=x&topic=x>, <mailto:unsubscribe@nutrition.co?subject=TopicUnsubscribe>")
                                        .build(),
                                MessageHeader.builder()
```

```
                                        .name("List-Unsubscribe-Post")
                                        .value("List-Unsubscribe=One-Click")
                                        .build()))
                        .build())
                .build();

        SendEmailRequest request = SendEmailRequest.builder()
                .fromEmailAddress(sender)
                .destination(d -> d.toAddresses(recipient))
                .content(emailContent)
                .build();

        try {
            SendEmailResponse response = sesv2Client.sendEmail(request);
            System.out.println("Email sent! Message ID: " +
 response.messageId());
        } catch (SesV2Exception e) {
            System.err.println("Failed to send email: " +
 e.awsErrorDetails().errorMessage());
            throw new RuntimeException(e);
        }
    }
}
```

- Einzelheiten zur API finden Sie SendEmailin der AWS SDK for Java 2.x API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Sendet eine Nachricht an alle Mitglieder der Kontaktliste.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
```

```
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
 Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")
```

Sendet mithilfe einer Vorlage eine Nachricht an alle Mitglieder der Kontaktliste.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email_address]},
                    Content={
                        "Template": {
                            "TemplateName": TEMPLATE_NAME,
                            "TemplateData": coupon_items,
                        }
                    },
                    ListManagementOptions={"ContactListName": CONTACT_LIST_NAME},
                )
```

- Einzelheiten zur API finden Sie SendEmailin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
require 'aws-sdk-sesv2'
require_relative 'config' # Recipient and sender email addresses.

# Set up the SESv2 client.
client = Aws::SESV2::Client.new(region: AWS_REGION)

def send_email(client, sender_email, recipient_email)
  response = client.send_email(
    {
      from_email_address: sender_email,
      destination: {
        to_addresses: [recipient_email]
      },
      content: {
        simple: {
          subject: {
            data: 'Test email subject'
          },
          body: {
            text: {
              data: 'Test email body'
            }
          }
        }
      }
    }
  )
  puts "Email sent from #{SENDER_EMAIL} to #{RECIPIENT_EMAIL} with message ID:
 #{response.message_id}"
end
```

```
send_email(client, SENDER_EMAIL, RECIPIENT_EMAIL)
```

- Einzelheiten zur API finden Sie SendEmailin der AWS SDK für Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Sendet eine Nachricht an alle Mitglieder der Kontaktliste.

```
async fn send_message(
    client: &Client,
    list: &str,
    from: &str,
    subject: &str,
    message: &str,
) -> Result<(), Error> {
    // Get list of email addresses from contact list.
    let resp = client
        .list_contacts()
        .contact_list_name(list)
        .send()
        .await?;

    let contacts = resp.contacts();

    let cs: Vec<String> = contacts
        .iter()
        .map(|i| i.email_address().unwrap_or_default().to_string())
        .collect();

    let mut dest: Destination = Destination::builder().build();
    dest.to_addresses = Some(cs);
    let subject_content = Content::builder()
```

```
        .data(subject)
        .charset("UTF-8")
        .build()
        .expect("building Content");
    let body_content = Content::builder()
        .data(message)
        .charset("UTF-8")
        .build()
        .expect("building Content");
    let body = Body::builder().text(body_content).build();

    let msg = Message::builder()
        .subject(subject_content)
        .body(body)
        .build();

    let email_content = EmailContent::builder().simple(msg).build();

    client
        .send_email()
        .from_email_address(from)
        .destination(dest)
        .content(email_content)
        .send()
        .await?;

    println!("Email sent to list");

    Ok(())
}
```

Sendet mithilfe einer Vorlage eine Nachricht an alle Mitglieder der Kontaktliste.

```
            let coupons = std::fs::read_to_string("../resources/newsletter/
sample_coupons.json")
                .unwrap_or_else(|_| r#"{"coupons":[]}"#.to_string());
            let email_content = EmailContent::builder()
                .template(
                    Template::builder()
                        .template_name(TEMPLATE_NAME)
                        .template_data(coupons)
                        .build(),
```

```
                )
                .build();

            match self
                .client
                .send_email()
                .from_email_address(self.verified_email.clone())

.destination(Destination::builder().to_addresses(email.clone()).build())
                .content(email_content)
                .list_management_options(
                    ListManagementOptions::builder()
                        .contact_list_name(CONTACT_LIST_NAME)
                        .build()?,
                )
                .send()
                .await
            {
                Ok(output) => {
                    if let Some(message_id) = output.message_id {
                        writeln!(
                            self.stdout,
                            "Newsletter sent to {} with message ID {}",
                            email, message_id
                        )?;
                    } else {
                        writeln!(self.stdout, "Newsletter sent to {}", email)?;
                    }
                }
                Err(e) => return Err(anyhow!("Error sending newsletter to {}:
{}", email, e)),
            }
```

- Einzelheiten zur API finden Sie SendEmailin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Sendet eine Nachricht.

```
    TRY.
        " Create destination with recipient address
        DATA lt_to_addresses TYPE /aws1/
cl_se2emailaddresslist_w=>tt_emailaddresslist.
        APPEND NEW /aws1/cl_se2emailaddresslist_w( iv_value =
 iv_to_email_address ) TO lt_to_addresses.
        DATA(lo_destination) = NEW /aws1/cl_se2destination(
          it_toaddresses = lt_to_addresses ).

        " Create message content
        DATA(lo_subject) = NEW /aws1/cl_se2content( iv_data = iv_subject ).
        DATA(lo_text_body) = NEW /aws1/cl_se2content( iv_data = iv_text_body ).
        DATA(lo_html_body) = NEW /aws1/cl_se2content( iv_data = iv_html_body ).
        DATA(lo_body) = NEW /aws1/cl_se2body(
          io_text = lo_text_body
          io_html = lo_html_body ).
        DATA(lo_message) = NEW /aws1/cl_se2message(
          io_subject = lo_subject
          io_body = lo_body ).

        DATA(lo_content) = NEW /aws1/cl_se2emailcontent(
          io_simple = lo_message ).

        " Send the email
        lo_se2->sendemail(
          iv_fromemailaddress = iv_from_email_address
          io_destination = lo_destination
          io_content = lo_content ).
        MESSAGE 'Email sent successfully.' TYPE 'I'.
      CATCH /aws1/cx_se2accountsuspendedex INTO DATA(lo_account_suspended).
        MESSAGE 'Account suspended.' TYPE 'I'.
```

```
        RAISE EXCEPTION lo_account_suspended.
      CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
        MESSAGE 'Bad request.' TYPE 'I'.
        RAISE EXCEPTION lo_bad_request.
      CATCH /aws1/cx_se2messagerejected INTO DATA(lo_message_rejected).
        MESSAGE 'Message rejected - check email verification.' TYPE 'I'.
        RAISE EXCEPTION lo_message_rejected.
    ENDTRY.
```

Sendet eine Nachricht unter Verwendung einer Vorlage.

```
    TRY.
        " Create destination with recipient address
        DATA lt_to_addresses TYPE /aws1/
cl_se2emailaddresslist_w=>tt_emailaddresslist.
        APPEND NEW /aws1/cl_se2emailaddresslist_w( iv_value =
 iv_to_email_address ) TO lt_to_addresses.
        DATA(lo_destination) = NEW /aws1/cl_se2destination(
          it_toaddresses = lt_to_addresses ).

        " Create template reference
        DATA(lo_template) = NEW /aws1/cl_se2template(
          iv_templatename = iv_template_name
          iv_templatedata = iv_template_data ).

        DATA(lo_content) = NEW /aws1/cl_se2emailcontent(
          io_template = lo_template ).

        " Create list management options
        DATA(lo_list_mgmt) = NEW /aws1/cl_se2listmanagementopts(
          iv_contactlistname = iv_contact_list_name ).

        " Send the email using template
        lo_se2->sendemail(
          iv_fromemailaddress = iv_from_email_address
          io_destination = lo_destination
          io_content = lo_content
          io_listmanagementoptions = lo_list_mgmt ).
        MESSAGE 'Email sent using template successfully.' TYPE 'I'.
      CATCH /aws1/cx_se2accountsuspendedex INTO DATA(lo_account_suspended).
        MESSAGE 'Account suspended.' TYPE 'I'.
        RAISE EXCEPTION lo_account_suspended.
```

```
      CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
        MESSAGE 'Bad request.' TYPE 'I'.
        RAISE EXCEPTION lo_bad_request.
      CATCH /aws1/cx_se2messagerejected INTO DATA(lo_message_rejected).
        MESSAGE 'Message rejected - check email verification.' TYPE 'I'.
        RAISE EXCEPTION lo_message_rejected.
    ENDTRY.
```

- Einzelheiten zur API finden Sie SendEmailin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Szenarien für die Verwendung von Amazon SES API v2 AWS SDKs

Die folgenden Codebeispiele zeigen Ihnen, wie Sie gängige Szenarien in Amazon SES API v2 mit implementieren AWS SDKs. Diese Szenarien zeigen Ihnen, wie Sie bestimmte Aufgaben durch den Aufruf mehrerer Funktionen innerhalb von Amazon SES API v2 oder in Kombination mit anderen AWS-Services ausführen können. Jedes Szenario enthält einen Link zum vollständigen Quell-Code, wo Sie Anleitungen zum Einrichten und Ausführen des Codes finden.

Szenarien zielen auf eine mittlere Erfahrungsebene ab, um Ihnen zu helfen, Service-Aktionen im Kontext zu verstehen.

Beispiele

- Ein vollständiges Amazon SES API v2-Newsletter-Szenario mit einem AWS SDK

Ein vollständiges Amazon SES API v2-Newsletter-Szenario mit einem AWS SDK

Die folgenden Codebeispiele zeigen, wie Sie das Newsletter-Szenario von Amazon SES API v2 ausführen.

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Führen Sie das Szenario aus.

```
using System.Diagnostics;
using System.Text.RegularExpressions;
using Amazon.SimpleEmailV2;
using Amazon.SimpleEmailV2.Model;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;
using Microsoft.Extensions.Logging;
using Microsoft.Extensions.Logging.Console;
using Microsoft.Extensions.Logging.Debug;

namespace Sesv2Scenario;

public static class NewsletterWorkflow
{
    /*
      This scenario demonstrates how to use the Amazon Simple Email Service (SES)
 v2 to send a coupon newsletter to a list of subscribers.
      The scenario performs the following tasks:

      1. Prepare the application:
         - Create a verified email identity for sending and replying to emails.
         - Create a contact list to store the subscribers' email addresses.
         - Create an email template for the coupon newsletter.

      2. Gather subscriber email addresses:
         - Prompt the user for a base email address.
         - Create 3 variants of the email address using subaddress extensions
 (e.g., user+ses-weekly-newsletter-1@example.com).
         - Add each variant as a contact to the contact list.
         - Send a welcome email to each new contact.
```

```
     3. Send the coupon newsletter:
        - Retrieve the list of contacts from the contact list.
        - Send the coupon newsletter using the email template to each contact.

     4. Monitor and review:
        - Provide instructions for the user to review the sending activity and
metrics in the AWS console.

     5. Clean up resources:
        - Delete the contact list (which also deletes all contacts within it).
        - Delete the email template.
        - Optionally delete the verified email identity.

   */

   public static SESv2Wrapper _sesv2Wrapper;
   public static string? _baseEmailAddress = null;
   public static string? _verifiedEmail = null;
   private static string _contactListName = "weekly-coupons-newsletter";
   private static string _templateName = "weekly-coupons";
   private static string _subject = "Weekly Coupons Newsletter";
   private static string _htmlContentFile = "coupon-newsletter.html";
   private static string _textContentFile = "coupon-newsletter.txt";
   private static string _htmlWelcomeFile = "welcome.html";
   private static string _textWelcomeFile = "welcome.txt";
   private static string _couponsDataFile = "sample_coupons.json";

   // Relative location of the resources folder.
   private static string _resourcesFilePathLocation = "../../../../resources/";

   public static async Task Main(string[] args)
   {
       // Set up dependency injection for the Amazon service.
       using var host = Host.CreateDefaultBuilder(args)
           .ConfigureLogging(logging =>
               logging.AddFilter("System", LogLevel.Debug)
                   .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                   .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
           .ConfigureServices((_, services) =>
               services.AddAWSService<IAmazonSimpleEmailServiceV2>()
                   .AddTransient<SESv2Wrapper>()
           )
```

```
            .Build();

        ServicesSetup(host);

        try
        {
            Console.WriteLine(new string('-', 80));
            Console.WriteLine(new string('-', 80));
            Console.WriteLine("Welcome to the Amazon SES v2 Coupon Newsletter
Scenario.");
            Console.WriteLine("This scenario demonstrates how to use the Amazon
Simple Email Service (SES) v2 " +
                              "\r\nto send a coupon newsletter to a list of
subscribers.");

            // Prepare the application.
            var emailIdentity = await PrepareApplication();

            // Gather subscriber email addresses.
            await GatherSubscriberEmailAddresses(emailIdentity);

            // Send the coupon newsletter.
            await SendCouponNewsletter(emailIdentity);

            // Monitor and review.
            MonitorAndReview(true);

            // Clean up resources.
            await Cleanup(emailIdentity, true);

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("Amazon SES v2 Coupon Newsletter scenario is
complete.");
            Console.WriteLine(new string('-', 80));
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred: {ex.Message}");
        }
    }

    /// <summary>
    /// Populate the services for use within the console application.
```

```
    /// </summary>
    /// <param name="host">The services host.</param>
    private static void ServicesSetup(IHost host)
    {
        _sesv2Wrapper = host.Services.GetRequiredService<SESv2Wrapper>();
    }

    /// <summary>
    /// Set up the resources for the scenario.
    /// </summary>
    /// <returns>The email address of the verified identity.</returns>
    public static async Task<string?> PrepareApplication()
    {
        var htmlContent = await File.ReadAllTextAsync(_resourcesFilePathLocation
+ _htmlContentFile);
        var textContent = await File.ReadAllTextAsync(_resourcesFilePathLocation
+ _textContentFile);

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("1. In this step, we will prepare the application:" +
                          "\r\n  - Create a verified email identity for sending
and replying to emails." +
                          "\r\n  - Create a contact list to store the
subscribers' email addresses." +
                          "\r\n  - Create an email template for the coupon
newsletter.\r\n");

        // Prompt the user for a verified email address.
        while (!IsEmail(_verifiedEmail))
        {
            Console.Write("Enter a verified email address or an email to verify:
");
            _verifiedEmail = Console.ReadLine();
        }

        try
        {
            // Create an email identity and start the verification process.
            await _sesv2Wrapper.CreateEmailIdentityAsync(_verifiedEmail);
            Console.WriteLine($"Identity {_verifiedEmail} created.");
        }
        catch (AlreadyExistsException)
        {
            Console.WriteLine($"Identity {_verifiedEmail} already exists.");
```

```
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating email identity: {ex.Message}");
        }

        // Create a contact list.
        try
        {
            await _sesv2Wrapper.CreateContactListAsync(_contactListName);
            Console.WriteLine($"Contact list {_contactListName} created.");
        }
        catch (AlreadyExistsException)
        {
            Console.WriteLine($"Contact list {_contactListName} already
exists.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating contact list: {ex.Message}");
        }

        // Create an email template.
        try
        {
            await _sesv2Wrapper.CreateEmailTemplateAsync(_templateName, _subject,
htmlContent, textContent);
            Console.WriteLine($"Email template {_templateName} created.");
        }
        catch (AlreadyExistsException)
        {
            Console.WriteLine($"Email template {_templateName} already exists.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating email template: {ex.Message}");
        }

        return _verifiedEmail;
    }

    /// <summary>
    /// Generate subscriber addresses and send welcome emails.
    /// </summary>
```

```
    /// <param name="fromEmailAddress">The verified email address from
 PrepareApplication.</param>
    /// <returns>True if successful.</returns>
    public static async Task<bool> GatherSubscriberEmailAddresses(string
 fromEmailAddress)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("2. In Step 2, we will gather subscriber email
 addresses:" +
                          "\r\n  - Prompt the user for a base email address." +
                          "\r\n  - Create 3 variants of the email address using
 subaddress extensions (e.g., user+ses-weekly-newsletter-1@example.com)." +
                          "\r\n  - Add each variant as a contact to the contact
 list." +
                          "\r\n  - Send a welcome email to each new contact.\r
\n");

        // Prompt the user for a base email address.
        while (!IsEmail(_baseEmailAddress))
        {
            Console.Write("Enter a base email address (e.g., user@example.com):
 ");
            _baseEmailAddress = Console.ReadLine();
        }

        // Create 3 variants of the email address using +ses-weekly-newsletter-1,
 +ses-weekly-newsletter-2, etc.
        var baseEmailAddressParts = _baseEmailAddress!.Split("@");
        for (int i = 1; i <= 3; i++)
        {
            string emailAddress = $"{baseEmailAddressParts[0]}+ses-weekly-
newsletter-{i}@{baseEmailAddressParts[1]}";

            try
            {
                // Create a contact with the email address in the contact list.
                await _sesv2Wrapper.CreateContactAsync(emailAddress,
 _contactListName);
                Console.WriteLine($"Contact {emailAddress} added to the
 {_contactListName} contact list.");
            }
            catch (AlreadyExistsException)
            {
```

```
                Console.WriteLine($"Contact {emailAddress} already exists in the
{_contactListName} contact list.");
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error creating contact {emailAddress}:
{ex.Message}");
                return false;
            }

            // Send a welcome email to the new contact.
            try
            {
                string subject = "Welcome to the Weekly Coupons Newsletter";
                string htmlContent = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _htmlWelcomeFile);
                string textContent = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _textWelcomeFile);

                await _sesv2Wrapper.SendEmailAsync(fromEmailAddress, new
List<string> { emailAddress }, subject, htmlContent, textContent);
                Console.WriteLine($"Welcome email sent to {emailAddress}.");
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error sending welcome email to
{emailAddress}: {ex.Message}");
                return false;
            }

            // Wait 2 seconds before sending the next email (if the account is in
the SES Sandbox).
            await Task.Delay(2000);
        }

        return true;
    }

    /// <summary>
    ///  Send the coupon newsletter to the subscribers in the contact list.
    /// </summary>
    /// <param name="fromEmailAddress">The verified email address from
PrepareApplication.</param>
    /// <returns>True if successful.</returns>
```

```
   public static async Task<bool> SendCouponNewsletter(string fromEmailAddress)
   {
       Console.WriteLine(new string('-', 80));
       Console.WriteLine("3. In this step, we will send the coupon newsletter:"
+
                         "\r\n  - Retrieve the list of contacts from the contact
list." +
                         "\r\n  - Send the coupon newsletter using the email
template to each contact.\r\n");


       // Retrieve the list of contacts from the contact list.
       var contacts = await _sesv2Wrapper.ListContactsAsync(_contactListName);
       if (!contacts.Any())
       {
           Console.WriteLine($"No contacts found in the {_contactListName}
contact list.");
           return false;
       }

       // Load the coupon data from the sample_coupons.json file.
       string couponsData = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _couponsDataFile);

       // Send the coupon newsletter to each contact using the email template.
       try
       {
           foreach (var contact in contacts)
           {
               // To use the Contact List for list management, send to only one
address at a time.
               await _sesv2Wrapper.SendEmailAsync(fromEmailAddress,
                   new List<string> { contact.EmailAddress },
                   null, null, null, _templateName, couponsData,
_contactListName);
           }

           Console.WriteLine($"Coupon newsletter sent to contact list
{_contactListName}.");
       }
       catch (Exception ex)
       {
           Console.WriteLine($"Error sending coupon newsletter to contact list
{_contactListName}: {ex.Message}");
```

```
            return false;
        }

        return true;
    }

    /// <summary>
    /// Provide instructions for monitoring sending activity and metrics.
    /// </summary>
    /// <param name="interactive">True to run in interactive mode.</param>
    /// <returns>True if successful.</returns>
    public static bool MonitorAndReview(bool interactive)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("4. In step 4, we will monitor and review:" +
                          "\r\n  - Provide instructions for the user to review
the sending activity and metrics in the AWS console.\r\n");

        Console.WriteLine("Review your sending activity using the SES Homepage in
the AWS console.");
        Console.WriteLine("Press Enter to open the SES Homepage in your default
browser...");
        if (interactive)
        {
            Console.ReadLine();
            try
            {
                // Open the SES Homepage in the default browser.
                Process.Start(new ProcessStartInfo
                {
                    FileName = "https://console.aws.amazon.com/ses/home",
                    UseShellExecute = true
                });
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error opening the SES Homepage:
{ex.Message}");
                return false;
            }
        }

        Console.WriteLine("Review the sending activity and email metrics, then
press Enter to continue...");
```

```
        if (interactive)
            Console.ReadLine();
        return true;
    }

    /// <summary>
    /// Clean up the resources used in the scenario.
    /// </summary>
    /// <param name="verifiedEmailAddress">The verified email address from
 PrepareApplication.</param>
    /// <param name="interactive">True if interactive.</param>
    /// <returns>Async task.</returns>
    public static async Task<bool> Cleanup(string verifiedEmailAddress, bool
 interactive)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("5. Finally, we clean up resources:" +
                          "\r\n  - Delete the contact list (which also deletes
 all contacts within it)." +
                          "\r\n  - Delete the email template." +
                          "\r\n  - Optionally delete the verified email identity.
\r\n");

        Console.WriteLine("Cleaning up resources...");

        // Delete the contact list (this also deletes all contacts in the list).
        try
        {
            await _sesv2Wrapper.DeleteContactListAsync(_contactListName);
            Console.WriteLine($"Contact list {_contactListName} deleted.");
        }
        catch (NotFoundException)
        {
            Console.WriteLine($"Contact list {_contactListName} not found.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error deleting contact list {_contactListName}:
 {ex.Message}");
            return false;
        }

        // Delete the email template.
        try
```

```
        {
            await _sesv2Wrapper.DeleteEmailTemplateAsync(_templateName);
            Console.WriteLine($"Email template {_templateName} deleted.");
        }
        catch (NotFoundException)
        {
            Console.WriteLine($"Email template {_templateName} not found.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error deleting email template {_templateName}:
{ex.Message}");
            return false;
        }

        // Ask the user if they want to delete the email identity.
        var deleteIdentity = !interactive ||
            GetYesNoResponse(
                $"Do you want to delete the email identity
{verifiedEmailAddress}? (y/n) ");
        if (deleteIdentity)
        {
            try
            {
                await
_sesv2Wrapper.DeleteEmailIdentityAsync(verifiedEmailAddress);
                Console.WriteLine($"Email identity {verifiedEmailAddress}
deleted.");
            }
            catch (NotFoundException)
            {
                Console.WriteLine(
                    $"Email identity {verifiedEmailAddress} not found.");
            }
            catch (Exception ex)
            {
                Console.WriteLine(
                    $"Error deleting email identity {verifiedEmailAddress}:
{ex.Message}");
                return false;
            }
        }
        else
        {
```

```
            Console.WriteLine(
                $"Skipping deletion of email identity {verifiedEmailAddress}.");
        }

        return true;
    }

    /// <summary>
    /// Helper method to get a yes or no response from the user.
    /// </summary>
    /// <param name="question">The question string to print on the console.</
param>
    /// <returns>True if the user responds with a yes.</returns>
    private static bool GetYesNoResponse(string question)
    {
        Console.WriteLine(question);
        var ynResponse = Console.ReadLine();
        var response = ynResponse != null && ynResponse.Equals("y",
 StringComparison.InvariantCultureIgnoreCase);
        return response;
    }

    /// <summary>
    /// Simple check to verify a string is an email address.
    /// </summary>
    /// <param name="email">The string to verify.</param>
    /// <returns>True if a valid email.</returns>
    private static bool IsEmail(string? email)
    {
        if (string.IsNullOrEmpty(email))
            return false;
        return Regex.IsMatch(email, @"^[^@\s]+@[^@\s]+\.[^@\s]+$",
 RegexOptions.IgnoreCase);
    }
}
```

Wrapper für Service-Vorgänge.

```
using System.Net;
using Amazon.SimpleEmailV2;
using Amazon.SimpleEmailV2.Model;
```

```
namespace Sesv2Scenario;

/// <summary>
/// Wrapper class for Amazon Simple Email Service (SES) v2 operations.
/// </summary>
public class SESv2Wrapper
{

    private readonly IAmazonSimpleEmailServiceV2 _sesClient;

    /// <summary>
    /// Constructor for the SESv2Wrapper.
    /// </summary>
    /// <param name="sesClient">The injected SES v2 client.</param>
    public SESv2Wrapper(IAmazonSimpleEmailServiceV2 sesClient)
    {
        _sesClient = sesClient;
    }

    /// <summary>
    /// Creates a contact and adds it to the specified contact list.
    /// </summary>
    /// <param name="emailAddress">The email address of the contact.</param>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>The response from the CreateContact operation.</returns>
    public async Task<bool> CreateContactAsync(string emailAddress, string
 contactListName)
    {
        var request = new CreateContactRequest
        {
            EmailAddress = emailAddress,
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.CreateContactAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Contact with email address {emailAddress} already
 exists in the contact list {contactListName}.");
            Console.WriteLine(ex.Message);
```

```
            return true;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the contact:
{ex.Message}");
        }
        return false;
    }

    /// <summary>
    /// Creates a contact list with the specified name.
    /// </summary>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateContactListAsync(string contactListName)
    {
        var request = new CreateContactListRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.CreateContactListAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Contact list with name {contactListName} already
exists.");
            Console.WriteLine(ex.Message);
```

```
            return true;
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for contact lists has been exceeded.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the contact
list: {ex.Message}");
        }
        return false;
    }

    /// <summary>
    /// Creates an email identity (email address or domain) and starts the
verification process.
    /// </summary>
    /// <param name="emailIdentity">The email address or domain to create and
verify.</param>
    /// <returns>The response from the CreateEmailIdentity operation.</returns>
    public async Task<CreateEmailIdentityResponse>
CreateEmailIdentityAsync(string emailIdentity)
    {
        var request = new CreateEmailIdentityRequest
        {
            EmailIdentity = emailIdentity
        };

        try
        {
            var response = await _sesClient.CreateEmailIdentityAsync(request);
            return response;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Email identity {emailIdentity} already exists.");
```

```
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} is being
modified by another operation or thread.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for email identities has been
exceeded.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} does not
exist.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the email
identity: {ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Creates an email template with the specified content.
    /// </summary>
    /// <param name="templateName">The name of the email template.</param>
    /// <param name="subject">The subject of the email template.</param>
```

```
    /// <param name="htmlContent">The HTML content of the email template.</param>
    /// <param name="textContent">The text content of the email template.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateEmailTemplateAsync(string templateName, string
subject, string htmlContent, string textContent)
    {
        var request = new CreateEmailTemplateRequest
        {
            TemplateName = templateName,
            TemplateContent = new EmailTemplateContent
            {
                Subject = subject,
                Html = htmlContent,
                Text = textContent
            }
        };

        try
        {
            var response = await _sesClient.CreateEmailTemplateAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Email template with name {templateName} already
exists.");
            Console.WriteLine(ex.Message);
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for email templates has been
exceeded.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the email
template: {ex.Message}");
```

```
        }

        return false;
    }

    /// <summary>
    /// Deletes a contact list and all contacts within it.
    /// </summary>
    /// <param name="contactListName">The name of the contact list to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteContactListAsync(string contactListName)
    {
        var request = new DeleteContactListRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.DeleteContactListAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The contact list {contactListName} is being
 modified by another operation or thread.");
            Console.WriteLine(ex.Message);
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
```

```
            Console.WriteLine($"An error occurred while deleting the contact
 list: {ex.Message}");
        }

        return false;
    }

    /// <summary>
    /// Deletes an email identity (email address or domain).
    /// </summary>
    /// <param name="emailIdentity">The email address or domain to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailIdentityAsync(string emailIdentity)
    {
        var request = new DeleteEmailIdentityRequest
        {
            EmailIdentity = emailIdentity
        };

        try
        {
            var response = await _sesClient.DeleteEmailIdentityAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} is being
 modified by another operation or thread.");
            Console.WriteLine(ex.Message);
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
```

```
        {
            Console.WriteLine($"An error occurred while deleting the email
 identity: {ex.Message}");
        }

        return false;
    }

    /// <summary>
    /// Deletes an email template.
    /// </summary>
    /// <param name="templateName">The name of the email template to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailTemplateAsync(string templateName)
    {
        var request = new DeleteEmailTemplateRequest
        {
            TemplateName = templateName
        };

        try
        {
            var response = await _sesClient.DeleteEmailTemplateAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email template {templateName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while deleting the email
 template: {ex.Message}");
        }
```

```
        return false;
    }

    /// <summary>
    /// Lists the contacts in the specified contact list.
    /// </summary>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>The list of contacts response from the ListContacts operation.</
returns>
    public async Task<List<Contact>> ListContactsAsync(string contactListName)
    {
        var request = new ListContactsRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.ListContactsAsync(request);
            return response.Contacts;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while listing the contacts:
 {ex.Message}");
        }

        return new List<Contact>();
    }

    /// <summary>
    /// Sends an email with the specified content and options.
```

```
    /// </summary>
    /// <param name="fromEmailAddress">The email address to send the email
from.</param>
    /// <param name="toEmailAddresses">The email addresses to send the email
to.</param>
    /// <param name="subject">The subject of the email.</param>
    /// <param name="htmlContent">The HTML content of the email.</param>
    /// <param name="textContent">The text content of the email.</param>
    /// <param name="templateName">The name of the email template to use
(optional).</param>
    /// <param name="templateData">The data to replace placeholders in the email
template (optional).</param>
    /// <param name="contactListName">The name of the contact list for
unsubscribe functionality (optional).</param>
    /// <returns>The MessageId response from the SendEmail operation.</returns>
    public async Task<string> SendEmailAsync(string fromEmailAddress,
List<string> toEmailAddresses, string? subject,
        string? htmlContent, string? textContent, string? templateName = null,
string? templateData = null, string? contactListName = null)
    {
        var request = new SendEmailRequest
        {
            FromEmailAddress = fromEmailAddress
        };

        if (toEmailAddresses.Any())
        {
            request.Destination = new Destination { ToAddresses =
toEmailAddresses };
        }

        if (!string.IsNullOrEmpty(templateName))
        {
            request.Content = new EmailContent()
            {
                Template = new Template
                {
                    TemplateName = templateName,
                    TemplateData = templateData
                }
            };
        }
        else
        {
```

```
            request.Content = new EmailContent
            {
                Simple = new Message
                {
                    Subject = new Content { Data = subject },
                    Body = new Body
                    {
                        Html = new Content { Data = htmlContent },
                        Text = new Content { Data = textContent }
                    }
                }
            };
        }

        if (!string.IsNullOrEmpty(contactListName))
        {
            request.ListManagementOptions = new ListManagementOptions
            {
                ContactListName = contactListName
            };
        }

        try
        {
            var response = await _sesClient.SendEmailAsync(request);
            return response.MessageId;
        }
        catch (AccountSuspendedException ex)
        {
            Console.WriteLine("The account's ability to send email has been
permanently restricted.");
            Console.WriteLine(ex.Message);
        }
        catch (MailFromDomainNotVerifiedException ex)
        {
            Console.WriteLine("The sending domain is not verified.");
            Console.WriteLine(ex.Message);
        }
        catch (MessageRejectedException ex)
        {
            Console.WriteLine("The message content is invalid.");
            Console.WriteLine(ex.Message);
        }
        catch (SendingPausedException ex)
```

```
        {
            Console.WriteLine("The account's ability to send email is currently
 paused.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while sending the email:
 {ex.Message}");
        }

        return string.Empty;
    }
}
```

- Weitere API-Informationen finden Sie in den folgenden Themen der AWS SDK für .NET - API-Referenz.
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail. einfach
  - SendEmail. Vorlage

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    try {
      // 2. Create a contact list
      String contactListName = CONTACT_LIST_NAME;
      CreateContactListRequest createContactListRequest =
 CreateContactListRequest.builder()
          .contactListName(contactListName)
          .build();
      sesClient.createContactList(createContactListRequest);
      System.out.println("Contact list created: " + contactListName);
    } catch (AlreadyExistsException e) {
      System.out.println("Contact list already exists, skipping creation: weekly-
coupons-newsletter");
    } catch (LimitExceededException e) {
      System.err.println("Limit for contact lists has been exceeded.");
      throw e;
    } catch (SesV2Exception e) {
      System.err.println("Error creating contact list: " + e.getMessage());
      throw e;
    }

      try {
        // Create a new contact with the provided email address in the
        CreateContactRequest contactRequest = CreateContactRequest.builder()
            .contactListName(CONTACT_LIST_NAME)
            .emailAddress(emailAddress)
            .build();

        sesClient.createContact(contactRequest);
        contacts.add(emailAddress);

        System.out.println("Contact created: " + emailAddress);
```

```
        // Send a welcome email to the new contact
        String welcomeHtml = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.html"));
        String welcomeText = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.txt"));

        SendEmailRequest welcomeEmailRequest = SendEmailRequest.builder()
            .fromEmailAddress(this.verifiedEmail)
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .simple(
                    Message.builder()
                        .subject(Content.builder().data("Welcome to the Weekly
 Coupons Newsletter").build())
                        .body(Body.builder()
                            .text(Content.builder().data(welcomeText).build())
                            .html(Content.builder().data(welcomeHtml).build())
                            .build())
                        .build())
                .build())
            .build();
        SendEmailResponse welcomeEmailResponse =
 sesClient.sendEmail(welcomeEmailRequest);
        System.out.println("Welcome email sent: " +
 welcomeEmailResponse.messageId());
      } catch (AlreadyExistsException e) {
        // If the contact already exists, skip this step for that contact and
 proceed
        // with the next contact
        System.out.println("Contact already exists, skipping creation...");
      } catch (Exception e) {
        System.err.println("Error occurred while processing email address " +
 emailAddress + ": " + e.getMessage());
        throw e;
      }
    }

      ListContactsRequest contactListRequest = ListContactsRequest.builder()
          .contactListName(CONTACT_LIST_NAME)
          .build();

      List<String> contactEmails;
      try {
```

```
        ListContactsResponse contactListResponse =
 sesClient.listContacts(contactListRequest);

        contactEmails = contactListResponse.contacts().stream()
            .map(Contact::emailAddress)
            .toList();
      } catch (Exception e) {
        // TODO: Remove when listContacts's GET body issue is resolved.
        contactEmails = this.contacts;
      }


      String coupons = Files.readString(Paths.get("resources/coupon_newsletter/
sample_coupons.json"));
      for (String emailAddress : contactEmails) {
        SendEmailRequest newsletterRequest = SendEmailRequest.builder()
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .template(Template.builder()
                    .templateName(TEMPLATE_NAME)
                    .templateData(coupons)
                    .build())
                .build())
            .fromEmailAddress(this.verifiedEmail)
            .listManagementOptions(ListManagementOptions.builder()
                .contactListName(CONTACT_LIST_NAME)
                .build())
            .build();
        SendEmailResponse newsletterResponse =
 sesClient.sendEmail(newsletterRequest);
        System.out.println("Newsletter sent to " + emailAddress + ": " +
 newsletterResponse.messageId());
      }

    try {
      CreateEmailIdentityRequest createEmailIdentityRequest =
 CreateEmailIdentityRequest.builder()
          .emailIdentity(verifiedEmail)
          .build();
      sesClient.createEmailIdentity(createEmailIdentityRequest);
      System.out.println("Email identity created: " + verifiedEmail);
    } catch (AlreadyExistsException e) {
      System.out.println("Email identity already exists, skipping creation: " +
 verifiedEmail);
```

```
    } catch (NotFoundException e) {
      System.err.println("The provided email address is not verified: " +
 verifiedEmail);
      throw e;
    } catch (LimitExceededException e) {
      System.err
          .println("You have reached the limit for email identities. Please
 remove some identities and try again.");
      throw e;
    } catch (SesV2Exception e) {
      System.err.println("Error creating email identity: " + e.getMessage());
      throw e;
    }

    try {
      // Create an email template named "weekly-coupons"
      String newsletterHtml = loadFile("resources/coupon_newsletter/coupon-
newsletter.html");
      String newsletterText = loadFile("resources/coupon_newsletter/coupon-
newsletter.txt");

      CreateEmailTemplateRequest templateRequest =
 CreateEmailTemplateRequest.builder()
          .templateName(TEMPLATE_NAME)
          .templateContent(EmailTemplateContent.builder()
              .subject("Weekly Coupons Newsletter")
              .html(newsletterHtml)
              .text(newsletterText)
              .build())
          .build();

      sesClient.createEmailTemplate(templateRequest);

      System.out.println("Email template created: " + TEMPLATE_NAME);
    } catch (AlreadyExistsException e) {
      // If the template already exists, skip this step and proceed with the next
      // operation
      System.out.println("Email template already exists, skipping creation...");
    } catch (LimitExceededException e) {
      // If the limit for email templates is exceeded, fail the workflow and
 inform
      // the user
      System.err.println("You have reached the limit for email templates. Please
 remove some templates and try again.");
```

```
      throw e;
    } catch (Exception e) {
      System.err.println("Error occurred while creating email template: " +
e.getMessage());
      throw e;
    }

    try {
      // Delete the contact list
      DeleteContactListRequest deleteContactListRequest =
DeleteContactListRequest.builder()
          .contactListName(CONTACT_LIST_NAME)
          .build();

      sesClient.deleteContactList(deleteContactListRequest);

      System.out.println("Contact list deleted: " + CONTACT_LIST_NAME);
    } catch (NotFoundException e) {
      // If the contact list does not exist, log the error and proceed
      System.out.println("Contact list not found. Skipping deletion...");
    } catch (Exception e) {
      System.err.println("Error occurred while deleting the contact list: " +
e.getMessage());
      e.printStackTrace();
    }

      try {
        // Delete the email identity
        DeleteEmailIdentityRequest deleteIdentityRequest =
DeleteEmailIdentityRequest.builder()
            .emailIdentity(this.verifiedEmail)
            .build();

        sesClient.deleteEmailIdentity(deleteIdentityRequest);

        System.out.println("Email identity deleted: " + this.verifiedEmail);
      } catch (NotFoundException e) {
        // If the email identity does not exist, log the error and proceed
        System.out.println("Email identity not found. Skipping deletion...");
      } catch (Exception e) {
        System.err.println("Error occurred while deleting the email identity: " +
e.getMessage());
        e.printStackTrace();
      }
```

```
    } else {
      System.out.println("Skipping email identity deletion.");
    }

    try {
      // Delete the template
      DeleteEmailTemplateRequest deleteTemplateRequest =
DeleteEmailTemplateRequest.builder()
          .templateName(TEMPLATE_NAME)
          .build();

      sesClient.deleteEmailTemplate(deleteTemplateRequest);

      System.out.println("Email template deleted: " + TEMPLATE_NAME);
    } catch (NotFoundException e) {
      // If the email template does not exist, log the error and proceed
      System.out.println("Email template not found. Skipping deletion...");
    } catch (Exception e) {
      System.err.println("Error occurred while deleting the email template: " +
e.getMessage());
      e.printStackTrace();
    }
```

- Weitere API-Informationen finden Sie in den folgenden Themen der AWS SDK for Java 2.x - API-Referenz.
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail. einfach
  - SendEmail. Vorlage

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.create_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' created successfully.")
```

```
        except ClientError as e:
            # If the contact list already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Contact list '{CONTACT_LIST_NAME}' already exists.")
            else:
                raise e

            try:
                # Create a new contact
                self.ses_client.create_contact(
                    ContactListName=CONTACT_LIST_NAME, EmailAddress=email
                )
                print(f"Contact with email '{email}' created successfully.")

                # Send the welcome email
                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")
                if self.sleep:
                    # 1 email per second in sandbox mode, remove in production.
                    sleep(1.1)
            except ClientError as e:
                # If the contact already exists, skip and proceed
                if e.response["Error"]["Code"] == "AlreadyExistsException":
                    print(f"Contact with email '{email}' already exists.
Skipping...")
                else:
                    raise e

        try:
```

```
            contacts_response = self.ses_client.list_contacts(
                ContactListName=CONTACT_LIST_NAME
            )
        except ClientError as e:
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
                return
            else:
                raise e

                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")

                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email_address]},
                    Content={
                        "Template": {
                            "TemplateName": TEMPLATE_NAME,
                            "TemplateData": coupon_items,
                        }
                    },
                    ListManagementOptions={"ContactListName": CONTACT_LIST_NAME},
                )

        try:

self.ses_client.create_email_identity(EmailIdentity=self.verified_email)
```

```
            print(f"Email identity '{self.verified_email}' created
successfully.")
        except ClientError as e:
            # If the email identity already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email identity '{self.verified_email}' already exists.")
            else:
                raise e

        try:
            template_content = {
                "Subject": "Weekly Coupons Newsletter",
                "Html": load_file_content("coupon-newsletter.html"),
                "Text": load_file_content("coupon-newsletter.txt"),
            }
            self.ses_client.create_email_template(
                TemplateName=TEMPLATE_NAME, TemplateContent=template_content
            )
            print(f"Email template '{TEMPLATE_NAME}' created successfully.")
        except ClientError as e:
            # If the template already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email template '{TEMPLATE_NAME}' already exists.")
            else:
                raise e

        try:

self.ses_client.delete_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' deleted successfully.")
        except ClientError as e:
            # If the contact list doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
            else:
                print(e)

            try:

self.ses_client.delete_email_identity(EmailIdentity=self.verified_email)
                print(f"Email identity '{self.verified_email}' deleted
successfully.")
            except ClientError as e:
                # If the email identity doesn't exist, skip and proceed
```

```
                if e.response["Error"]["Code"] == "NotFoundException":
                    print(f"Email identity '{self.verified_email}' does not
exist.")
                else:
                    print(e)

        try:
            self.ses_client.delete_email_template(TemplateName=TEMPLATE_NAME)
            print(f"Email template '{TEMPLATE_NAME}' deleted successfully.")
        except ClientError as e:
            # If the email template doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Email template '{TEMPLATE_NAME}' does not exist.")
            else:
                print(e)
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Python (Boto3).
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail. einfach
  - SendEmail. Vorlage

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
        match self
            .client
            .create_contact_list()
            .contact_list_name(CONTACT_LIST_NAME)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Contact list created
successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateContactListError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Contact list already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating contact list: {}", e)),
            },
        }

            match self
                .client
                .create_contact()
                .contact_list_name(CONTACT_LIST_NAME)
                .email_address(email.clone())
                .send()
                .await
            {
                Ok(_) => writeln!(self.stdout, "Contact created for {}", email)?,
                Err(e) => match e.into_service_error() {
                    CreateContactError::AlreadyExistsException(_) => writeln!(
                        self.stdout,
```

```
                        "Contact already exists for {}, skipping creation.",
                        email
                    )?,
                    e => return Err(anyhow!("Error creating contact for {}: {}",
 email, e)),
                },
            }

        let contacts: Vec<Contact> = match self
            .client
            .list_contacts()
            .contact_list_name(CONTACT_LIST_NAME)
            .send()
            .await
        {
            Ok(list_contacts_output) => {
                list_contacts_output.contacts.unwrap().into_iter().collect()
            }
            Err(e) => {
                return Err(anyhow!(
                    "Error retrieving contact list {}: {}",
                    CONTACT_LIST_NAME,
                    e
                ))
            }
        };

            let coupons = std::fs::read_to_string("../resources/newsletter/
sample_coupons.json")
                .unwrap_or_else(|_| r#"{"coupons":[]}"#.to_string());
            let email_content = EmailContent::builder()
                .template(
                    Template::builder()
                        .template_name(TEMPLATE_NAME)
                        .template_data(coupons)
                        .build(),
                )
                .build();

            match self
                .client
                .send_email()
                .from_email_address(self.verified_email.clone())
```

```
.destination(Destination::builder().to_addresses(email.clone()).build())
                .content(email_content)
                .list_management_options(
                    ListManagementOptions::builder()
                        .contact_list_name(CONTACT_LIST_NAME)
                        .build()?,
                )
                .send()
                .await
            {
                Ok(output) => {
                    if let Some(message_id) = output.message_id {
                        writeln!(
                            self.stdout,
                            "Newsletter sent to {} with message ID {}",
                            email, message_id
                        )?;
                    } else {
                        writeln!(self.stdout, "Newsletter sent to {}", email)?;
                    }
                }
                Err(e) => return Err(anyhow!("Error sending newsletter to {}:
{}", email, e)),
            }

        match self
            .client
            .create_email_identity()
            .email_identity(self.verified_email.clone())
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email identity created
successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateEmailIdentityError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Email identity already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating email identity: {}", e)),
            },
```

```
        }

        let template_html =
            std::fs::read_to_string("../resources/newsletter/coupon-
newsletter.html")
                .unwrap_or_else(|_| "Missing coupon-
newsletter.html".to_string());
        let template_text =
            std::fs::read_to_string("../resources/newsletter/coupon-
newsletter.txt")
                .unwrap_or_else(|_| "Missing coupon-newsletter.txt".to_string());

        // Create the email template
        let template_content = EmailTemplateContent::builder()
            .subject("Weekly Coupons Newsletter")
            .html(template_html)
            .text(template_text)
            .build();

        match self
            .client
            .create_email_template()
            .template_name(TEMPLATE_NAME)
            .template_content(template_content)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email template created
 successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateEmailTemplateError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Email template already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating email template: {}", e)),
            },
        }

        match self
            .client
            .delete_contact_list()
            .contact_list_name(CONTACT_LIST_NAME)
```

```
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Contact list deleted
successfully.")?,
            Err(e) => return Err(anyhow!("Error deleting contact list: {e}")),
        }

            match self
                .client
                .delete_email_identity()
                .email_identity(self.verified_email.clone())
                .send()
                .await
            {
                Ok(_) => writeln!(self.stdout, "Email identity deleted
successfully.")?,
                Err(e) => {
                    return Err(anyhow!("Error deleting email identity: {}", e));
                }
            }

        match self
            .client
            .delete_email_template()
            .template_name(TEMPLATE_NAME)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email template deleted
successfully.")?,
            Err(e) => {
                return Err(anyhow!("Error deleting email template: {e}"));
            }
        }
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Rust.
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity

- CreateEmailTemplate
- DeleteContactList
- DeleteEmailIdentity
- DeleteEmailTemplate
- ListContacts
- SendEmail. einfach
- SendEmail. Vorlage

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterAmazon SES mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Amazon Simple Email Service

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon Simple Email Service gelten, finden Sie unter AWS Services in Umfang nach Compliance-ProgrammAWS unter .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation zeigt Ihnen, wie Sie das Modell der übergreifenden Verantwortlichkeit bei der Verwendung von Amazon EC2 einsetzen können. Es zeigt Ihnen, wie Sie Amazon EC2 konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Amazon Simple Email Service-Ressourcen zu überwachen und zu sichern.

> **Note**
>
> Wenn Sie Missbrauch von AWS Ressourcen melden müssen, einschließlich E-Mail-Spam und Verbreitung von Malware, verwenden Sie nicht den Feedback-Link auf einer der Seiten dieses Entwicklerhandbuchs, da das Formular vom AWS Dokumentationsteam und nicht von AWS Trust & Safety eingegangen ist. Stattdessen auf der Seite Wie melde ich Missbrauch von AWS Ressourcen? Seite, folgen Sie den Anweisungen, um das AWS Trust & Safety Team zu kontaktieren, um jegliche Art von AWS Missbrauch durch Amazon zu melden.

Inhalt

- Datenschutz in Amazon Simple Email Service
- Identity and Access Management in Amazon S3
- Protokollierung und Überwachung in Amazon SES
- Compliance-Validierung für Amazon Simple Email Service
- Amazon Simple Email Service
- Sicherheit der Infrastruktur in Amazon OpenSearch Service
- Einrichten von VPC-Endpunkten mit Amazon SES

Datenschutz in Amazon Simple Email Service

Das AWS Modell der gilt für den Datenschutz in Amazon Simple Email Service. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.

- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon Simple Email Service oder anderen AWS-Services über die Konsole AWS CLI, API oder arbeiten AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Inhalt

- Datenverschlüsselung im Ruhezustand für Amazon SES
- Verschlüsselung während der Übertragung
- Löschen personenbezogener Daten aus Amazon SES

Datenverschlüsselung im Ruhezustand für Amazon SES

Standardmäßig verschlüsselt Amazon SES alle Daten im Ruhezustand. Die standardmäßige Verschlüsselung trägt dazu bei, den betrieblichen Aufwand und die Komplexität des Datenschutzes zu reduzieren. Mithilfe der Verschlüsselung können Sie auch Mail Manager-Archive erstellen, die den strengen Verschlüsselungsvorschriften und gesetzlichen Anforderungen entsprechen.

SES bietet die folgenden Verschlüsselungsoptionen:

- AWS eigene Schlüssel — SES verwendet diese standardmäßig. Sie können AWS eigene Schlüssel nicht einsehen, verwalten oder verwenden oder deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme zum Schutz der Schlüssel ändern, die zur Verschlüsselung Ihrer Daten verwendet werden. Weitere Informationen finden Sie unter AWS -eigene Schlüssel im AWS Key Management Service -Entwicklerhandbuch.
- Vom Kunden verwaltete Schlüssel — SES unterstützt die Verwendung symmetrischer, vom Kunden verwalteter Schlüssel, die Sie erstellen, besitzen und verwalten. Da Sie die volle Kontrolle über die Verschlüsselung haben, können Sie beispielsweise folgende Aufgaben ausführen:

- Festlegung und Pflege wichtiger Richtlinien
- Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
- Aktivieren und Deaktivieren wichtiger Richtlinien
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von -Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen

Um Ihren eigenen Schlüssel zu verwenden, wählen Sie bei der Erstellung Ihrer SES-Ressourcen einen vom Kunden verwalteten Schlüssel aus.

Weitere Informationen finden Sie unter Kundenverwaltete Schlüssel im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> SES aktiviert automatisch und kostenlos die Verschlüsselung im Ruhezustand mithilfe AWS eigener Schlüssel.
> Für die Verwendung eines vom Kunden verwalteten Schlüssels fallen jedoch AWS KMS Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter AWS Key Management Service Preisgestaltung.

Erstellen eines kundenseitig verwalteten Schlüssels

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen, indem Sie den AWS-Managementkonsole, oder den AWS KMS APIs verwenden.

Einen symmetrischen kundenverwalteten Schlüssel erstellen

Befolgen Sie die Schritte zur Erstellung von KMS-Schlüsseln mit symmetrischer Verschlüsselung im AWS Key Management Service -Entwicklerhandbuch.

> **Note**
>
> Für die Archivierung muss Ihr Schlüssel die folgenden Anforderungen erfüllen:
>
> - Der Schlüssel muss symmetrisch sein.

- Der wichtigste Materialursprung muss sein`AWS_KMS`.
- Die Schlüsselverwendung muss sein`ENCRYPT_DECRYPT`.

Schlüsselrichtlinie

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren kundenseitig verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf kundenverwaltete Schlüssel im Entwicklerhandbuch zum AWS Key Management Service .

Um Ihren vom Kunden verwalteten Schlüssel mit der Mail Manager-Archivierung zu verwenden, muss Ihre Schlüsselrichtlinie die folgenden API-Operationen zulassen:

- kms: DescribeKey — Stellt dem Kunden die vom Kunden verwalteten Schlüssel bereit, die es SES ermöglichen, den Schlüssel zu validieren.
- kms: GenerateDataKey — Ermöglicht SES, einen Datenschlüssel für die Verschlüsselung von Daten im Ruhezustand zu generieren.
- kms:Decrypt — Ermöglicht SES, gespeicherte Daten zu entschlüsseln, bevor sie an API-Clients zurückgegeben werden.

Das folgende Beispiel zeigt eine typische Schlüsselrichtlinie:

```
{
            "Sid": "Allow SES to encrypt/decrypt",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
```

Weitere Informationen finden Sie im AWS Key Management Service Entwicklerhandbuch unter Angeben von Berechtigungen in einer Richtlinie.

Weitere Informationen zur Problembehandlung finden Sie im AWS Key Management Service Entwicklerhandbuch unter Problembehandlung beim Schlüsselzugriff.

Einen vom Kunden verwalteten Schlüssel für Mail Manager angeben

Sie können einen vom Kunden verwalteten Schlüssel als Alternative zur Verwendung AWS eigener Schlüssel angeben. Wenn Sie ein Archiv erstellen oder einen Eingangsendpunkt mit gegenseitiger TLS-Authentifizierung (mTLS) konfigurieren, können Sie den Datenschlüssel angeben, indem Sie einen KMS-Schlüssel-ARN eingeben. Bei der Archivierung verwendet Mail Manager den Schlüssel, um alle Kundendaten im Archiv zu verschlüsseln. Bei mTLS-Eingangsendpunkten verwendet Mail Manager den Schlüssel, um den Inhalt des Trust-Stores im Ruhezustand zu verschlüsseln.

- KMS-Schlüssel-ARN — Eine Schlüssel-ID für einen vom AWS KMS Kunden verwalteten Schlüssel. Geben Sie eine Schlüssel-ID, einen Schlüssel-ARN, einen Alias-Namen oder einen Alias-ARN ein.

Amazon-SES-Verschlüsselungskontext

Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, die zusätzliche kontextbezogene Informationen zu den Daten enthalten.

AWS KMS verwendet den Verschlüsselungskontext als zusätzliche authentifizierte Daten, um die authentifizierte Verschlüsselung zu unterstützen. Wenn Sie einen Verschlüsselungskontext in eine Anforderung zum Verschlüsseln von Daten einbeziehen, wird der Verschlüsselungskontext AWS KMS an die verschlüsselten Daten gebunden. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben.

> **Note**
>
> Amazon SES unterstützt keine Verschlüsselungskontexte für die Archivierungserstellung. Stattdessen verwenden Sie eine IAM- oder KMS-Richtlinie. Richtlinien finden Sie Richtlinien für die Erstellung von Archiven beispielsweise weiter unten in diesem Abschnitt.

Amazon SES SES-Verschlüsselungskontext

SES verwendet bei allen AWS KMS kryptografischen Vorgängen denselben Verschlüsselungskontext, wobei der Schlüssel `aws:ses:arn` und der Wert die Ressource Amazon Resource Name (ARN) ist.

Example

```
"encryptionContext": {
    "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
}
```

Verwenden des Verschlüsselungskontexts für die Überwachung

Wenn Sie einen symmetrischen, vom Kunden verwalteten Schlüssel zur Verschlüsselung Ihrer SES-Ressource verwenden, können Sie den Verschlüsselungskontext auch in Prüfaufzeichnungen und Protokollen verwenden, um festzustellen, wie der vom Kunden verwaltete Schlüssel verwendet wird. Der Verschlüsselungskontext erscheint auch in Protokollen, die von Amazon CloudWatch Logs generiert wurden AWS CloudTrail.

Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf den vom Kunden verwalteten Schlüssel

Sie können den Verschlüsselungskontext in Schlüsselrichtlinien und IAM-Richtlinien als `conditions` verwenden, um den Zugriff auf Ihren symmetrischen, kundenverwalteten Schlüssel zu kontrollieren. Sie können Verschlüsselungskontext-Einschränkungen auch in einer Genehmigung verwenden.

SES verwendet bei Zuschüssen eine Einschränkung des Verschlüsselungskontextes, um den Zugriff auf den vom Kunden verwalteten Schlüssel in Ihrem Konto oder Ihrer Region zu kontrollieren. Eine Genehmigungseinschränkung erfordert, dass durch die Genehmigung ermöglichte Vorgänge den angegebenen Verschlüsselungskontext verwenden.

Example

Im Folgenden finden Sie Beispiele für Schlüsselrichtlinienanweisungen zur Gewährung des Zugriffs auf einen kundenseitig verwalteten Schlüssel für einen bestimmten Verschlüsselungskontext. Die Bedingung in dieser Richtlinienanweisung setzt voraus, dass die Genehmigungen eine Einschränkung des Verschlüsselungskontextes haben, die den Verschlüsselungskontext spezifiziert.

```
{
    "Sid": "Enable DescribeKey",
```

```
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:DescribeKey",
     "Resource": "*"
},
{
     "Sid": "Enable CreateGrant",
     "Effect": "Allow",
     "Principal": {
         "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:CreateGrant",
     "Resource": "*",
     "Condition": {
         "StringEquals": {
             "kms:EncryptionContext:aws:ses:arn": "arn:aws:ses:us-
west-2:111122223333:ExampleResourceName/ExampleResourceID"
          }
     }
}
```

Richtlinien für die Erstellung von Archiven

Die folgenden Beispielrichtlinien zeigen, wie die Archivierungserstellung aktiviert wird. Die Richtlinien gelten für alle Ressourcen.

IAM-Richtlinie

```
{
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ses:CreateArchive",
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
```

```
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ses.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "012345678910"
                }
            }
        }
```

AWS KMS Richtlinie

```
{
            "Sid": "Allow SES to encrypt/decrypt",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
```

mTLS-Richtlinien für Eingangsendpunkte

Die folgenden Beispielrichtlinien ermöglichen die Verwendung eines vom Kunden verwalteten Schlüssels zur Verschlüsselung von Trust Store-Inhalten für die gegenseitige TLS-Authentifizierung (mTLS) auf Mail Manager-Eingangsendpunkten.

Um die Beispielrichtlinien auf einen bestimmten Eingangsendpunkt zu beschränken, ersetzen Sie den Platzhalter in der Bedingung durch einen exakten Ressourcen-ARN (z. B.`arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/inp-ab1c2defgh3ij4klmno5pq6rs`).

IAM-Richtlinie

```
{
    "Effect": "Allow",
```

```
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/rolename"
    },
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "ses.us-east-1.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:ses:arn": [
          "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/*"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/rolename"
    },
    "Action": [
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "ses.us-east-1.amazonaws.com"
      }
    }
  }
```

AWS KMS Richtlinie

```
{
    "Effect": "Allow",
    "Principal": {
      "Service": "ses.amazonaws.com"
    },
    "Action": [
```

```
      "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "aws:SourceArn": [
          "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/*"
        ],
        "kms:EncryptionContext:aws:ses:arn": [
          "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/*"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "ses.amazonaws.com"
    },
    "Action": [
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "aws:SourceArn": [
          "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/*"
        ]
      }
    }
  }
```

Überwachung Ihrer Verschlüsselungsschlüssel für Amazon SES

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel mit Ihren Amazon SES SES-Ressourcen verwenden, können Sie Amazon CloudWatch Logs verwenden AWS CloudTrail, um Anfragen zu verfolgen, an die SES sendet AWS KMS.

Die folgenden Beispiele sind AWS CloudTrail Ereignisse für`GenerateDataKey`, und `DescribeKey` zur Überwachung von KMS-Vorgängen`Decrypt`, die von SES aufgerufen werden, um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden:

GenerateDataKey

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel für Ihre Ressource aktivieren, erstellt SES einen eindeutigen Tabellenschlüssel. Es sendet eine `GenerateDataKey` Anfrage an AWS KMS , in der der vom AWS KMS Kunden verwaltete Schlüssel für die Ressource angegeben wird.

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel für Ihre Mail Manager-Archivressource aktivieren, wird dieser `GenerateDataKey` beim Verschlüsseln von Archivdaten im Ruhezustand verwendet.

Das folgende Beispielereignis zeichnet den Vorgang `GenerateDataKey` auf:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "ses.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
        },
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "57f5dbee-16da-413e-979f-2c4c6663475e"
}
```

Decrypt

Wenn Sie auf eine verschlüsselte Ressource zugreifen, ruft SES den `Decrypt` Vorgang auf, um den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf die verschlüsselten Daten zu verwenden.

Das folgende Beispielereignis zeichnet den Vorgang `Decrypt` auf:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "ses.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:10:51Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
```

```
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "dc129381-1d94-49bd-b522-f56a3482d088"
}
```

DescribeKey

SES überprüft anhand des `DescribeKey` Vorgangs, ob der mit Ihrer Ressource verknüpfte, vom AWS KMS Kunden verwaltete Schlüssel im Konto und in der Region existiert.

Das folgende Beispielereignis zeichnet den Vorgang `DescribeKey` auf:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
```

```
            }
        },
        "invokedBy": "ses.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


Weitere Informationen

Die folgenden Ressourcen enthalten weitere Informationen zur Datenverschlüsselung im Ruhezustand:

- Weitere Informationen zu grundlegenden AWS Key Management Service -Konzepten finden Sie im AWS Key Management Service -Entwicklerhandbuch.
- Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit AWS Key Management Service im AWS Key Management Service -Entwicklerhandbuch.

Verschlüsselung während der Übertragung

Standardmäßig verwendet Amazon SES opportunistische TLS. Das bedeutet, dass Amazon SES immer versucht, eine sichere Verbindung mit dem empfangenden Mail-Server herzustellen. Wenn keine sichere Verbindung herstellen kann, wird die Nachricht unverschlüsselt gesendet. Sie können dieses Verhalten so ändern, dass Amazon SES die Nachricht nur dann zum empfangenden E-Mail-Server sendet, wenn eine sichere Verbindung hergestellt werden kann. Weitere Informationen finden Sie unter Amazon SES und Sicherheitsprotokolle.

Löschen personenbezogener Daten aus Amazon SES

Abhängig davon, wie Sie Amazon SES verwenden, werden möglicherweise Daten gespeichert, die als personenbezogen angesehen werden könnten. Um beispielsweise E-Mails mit Amazon SES versenden zu können, müssen Sie mindestens eine verifizierte Identität (eine E-Mail-Adresse oder eine Domäne) angeben. Sie können diese personenbezogenen Daten über die Amazon SES-Konsole oder die Amazon SES-API permanent löschen.

Dieses Kapitel enthält Verfahren zum Löschen verschiedener Arten von Daten, die als personenbezogen angesehen werden könnten.

Inhalt

- Löschen von E-Mail-Adressen aus der Unterdrückungsliste auf Kontoebene
- Löschen von Daten zu mit Amazon SES gesendeten E-Mails
- Löschen von Daten über Identitäten
- Löschen von Absender-Authentifizierungsdaten
- Löschen von auf Empfangsregeln bezogenen Daten
- Löschen von auf IP-Adressfilter bezogenen Daten
- Löschen von Daten in E-Mail-Vorlagen
- Löschen von Daten in benutzerdefinierten Vorlagen zur E-Mail-Verifizierung
- Löschen Sie alle persönlichen Daten, indem Sie Ihr AWS Konto schließen

Löschen von E-Mail-Adressen aus der Unterdrückungsliste auf Kontoebene

Amazon SES enthält eine optionale Unterdrückungsliste auf Kontoebene. Wenn Sie diese Funktion aktivieren, werden E-Mail-Adressen automatisch zu einer Unterdrückungsliste hinzugefügt, wenn

sie zu einer Unzustellbarkeit oder Beschwerde führen. E-Mail-Adressen bleiben so lange auf dieser Liste, bis Sie sie löschen. Weitere Hinweise zur Unterdrückungsliste auf Kontoebene finden Sie unter Verwenden der Unterdrückungsliste auf Kontoebene der Amazon-SES-Konsole.

Sie können E-Mail-Adressen aus der Unterdrückungsliste auf Kontoebene löschen, indem Sie die `DeleteSuppressedDestination`-Operation unter Amazon SES-API v2 nutzen. Dieser Abschnitt enthält ein Verfahren zum Löschen von E-Mail-Adressen mithilfe der AWS CLI. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im AWS Command Line Interface - Benutzerhandbuch.

Um eine Adresse aus der Unterdrückungsliste auf Kontoebene zu entfernen, verwenden Sie den AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws sesv2 delete-suppressed-destination --email-address recipient@example.com
  ```

  Ersetzen Sie im vorherigen Befehl *recipient@example.com* durch die E-Mail-Adresse, die Sie aus der Unterdrückungsliste auf Kontoebene entfernen möchten.

Löschen von Daten zu mit Amazon SES gesendeten E-Mails

Wenn Sie Amazon SES verwenden, um eine E-Mail zu senden, können Sie Informationen zu dieser E-Mail an andere AWS Dienste senden. Sie können beispielsweise Informationen über E-Mail-Ereignisse (wie Lieferungen, Öffnungen und Klicks) an Firehose senden. Diese Ereignisdaten enthalten in der Regel Ihre E-Mail-Adresse und die IP-Adresse, über die die E-Mail gesendet wurde. Außerdem enthalten Sie die E-Mail-Adressen aller Empfänger, an die die E-Mail gesendet wurde.

Sie können Firehose verwenden, um E-Mail-Ereignisdaten an mehrere Ziele zu streamen, darunter Amazon Simple Storage Service, Amazon Service und Amazon OpenSearch Redshift. Um diese Daten zu entfernen, sollten Sie zuerst das Streamen von Daten zu Firehose beenden und dann die Daten löschen, die bereits gestreamt wurden. Um das Streamen von Amazon SES SES-Ereignisdaten an Firehose zu beenden, müssen Sie das Firehose-Ereignisziel löschen.

So entfernen Sie ein Firehose-Ereignisziel mithilfe der Amazon SES SES-Konsole

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie unter Email Sending (E-Mail-Versand) Configuration Sets (Konfigurationssätze) aus.

3. Wählen Sie in der Liste der Konfigurationssätze den Konfigurationssatz aus, der das Firehose-Ereignisziel enthält.
4. Wählen Sie neben dem Firehose-Ereignisziel, das Sie löschen möchten, die Schaltfläche Löschen
   ( ).
5. Entfernen Sie gegebenenfalls die Daten, die Firehose an andere Dienste geschrieben hat. Weitere Informationen finden Sie unter the section called “Entfernen gespeicherter Ereignisdaten”.

Ereignisziele können auch mithilfe der Amazon SES-API gelöscht werden. Das folgende Verfahren verwendet die AWS Command Line Interface (AWS CLI), um mit der Amazon SES SES-API zu interagieren. Sie können auch mit der API interagieren, indem Sie ein AWS SDK verwenden oder HTTP-Anfragen direkt stellen.

Um ein Firehose-Ereignisziel zu entfernen, verwenden Sie den AWS CLI

1. Geben Sie in der Befehlszeile folgenden Befehl ein:

   ```
   aws sesv2 delete-configuration-set-event-destination --configuration-set-
   name configSet \
   --event-destination-name eventDestination
   ```

   Ersetzen Sie in diesem Befehl *configSet* durch den Namen des Konfigurationssatzes, der das Firehose-Ereignisziel enthält. *eventDestination*Ersetzen Sie durch den Namen des Firehose-Ereignisziels.
2. Entfernen Sie gegebenenfalls die Daten, die Firehose an andere Dienste geschrieben hat. Weitere Informationen finden Sie unter the section called “Entfernen gespeicherter Ereignisdaten”.

Entfernen gespeicherter Ereignisdaten

Weitere Informationen zum Löschen von Informationen aus anderen AWS Diensten finden Sie in den folgenden Dokumenten:

- Objekt und Bucket löschenimLeitfaden „Erste Schritte“ für Amazon Simple Storage Service
- Löschen Sie eine OpenSearch Service-Domain im Amazon OpenSearch Service Developer Guide
- Löschen eines Clusters im Amazon Redshift Cluster-Managementleitfaden

Sie können Firehose auch verwenden, um E-Mail-Daten an Splunk zu streamen, einen Drittanbieterdienst, der nicht von der unterstützt AWS oder verwaltet wird. AWS-Managementkonsole Wenden Sie sich für weitere Informationen zum Entfernen von Daten aus Splunk an Ihren Systemadministrator oder konsultieren Sie die Dokumentation auf der Splunk-Website.

Löschen von Daten über Identitäten

Identitäten umfassen die E-Mail-Adressen und Domänen, die Sie beim Senden von E-Mails mithilfe von Amazon SES verwenden. In einigen Jurisdiktionen werden möglicherweise E-Mail-Adressen oder Domänen als personenbezogene Informationen angesehen.

So löschen Sie eine Identität mithilfe der Amazon SES-Konsole

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Führen Sie unter Identity Management (Identitätsverwaltung) einen der folgenden Schritte aus:
   - Wählen Sie Domains (Domäne), wenn Sie eine Domäne löschen möchten.
   - Wählen Sie Email Addresses (E-Mail-Adressen), wenn Sie eine E-Mail-Adresse löschen möchten.
3. Wählen Sie die Identität aus, die Sie löschen möchten, und klicken Sie auf Remove (Entfernen).
4. Wählen Sie im Bestätigungsdialogfeld Yes, Delete Identität (Ja, Identität löschen) aus.

Identitäten können auch mithilfe der Amazon SES-API gelöscht werden. Im folgenden Verfahren wird die AWS Command Line Interface (AWS CLI) für die Interaktion mit der Amazon SES-API verwendet. Sie können auch mit der API interagieren, indem Sie ein AWS SDK verwenden oder direkt HTTP-Anfragen stellen.

Um eine Identität mit dem zu löschen AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws ses delete-identity --identity sender@example.com
  ```

  Ersetzen Sie in diesem Befehl *sender@example.com* durch die Identität, die Sie löschen möchten.

Löschen von Absender-Authentifizierungsdaten

Absenderauthentifizierung bezieht sich auf den Vorgang, mit dem Amazon SES so konfiguriert wird, dass andere Benutzer in Ihrem Namen E-Mails senden können. Zum Aktivieren der Absenderautorisierung müssen Sie nach der Beschreibung in Verwenden der Sendeautorisierung mit Amazon SES eine Richtlinie erstellen. Diese Richtlinien enthalten zusätzlich zu (die der Person oder Gruppe zugeordnet sind, die in Ihrem Namen E-Mails sendet) Identitäten AWS IDs (die Ihnen gehören). Sie können diese personenbezogenen Daten durch Ändern oder Löschen der Absenders-Authentifizierungsrichtlinien löschen. Die folgenden Verfahren beschreiben, wie Sie diese Richtlinien löschen.

So löschen Sie eine Absender-Authentifizierungsrichtlinie mithilfe der Amazon SES-Konsole

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Führen Sie unter Identity Management (Identitätsverwaltung) einen der folgenden Schritte aus:
   - Wählen Sie Domains (Domänen), wenn die Absender-Authentifizierungsrichtlinie, die Sie löschen möchten, einer Domäne zugeordnet ist.
   - Wählen Sie Email Addresses (E-Mail-Adressen), wenn die Absender-Authentifizierungsrichtlinie, die Sie löschen möchten, einer E-Mail-Adresse zugeordnet ist.
3. Wählen Sie unter Identity Policies (Identitätsrichtlinien) die Richtlinie aus, die Sie löschen möchten, und klicken Sie dann auf Remove Policy (Richtlinie entfernen).

Absender-Authentifizierungsrichtlinien können auch mithilfe der Amazon SES-API gelöscht werden. Das folgende Verfahren verwendet die AWS Command Line Interface (AWS CLI), um mit der Amazon SES SES-API zu interagieren. Sie können auch mit der API interagieren, indem Sie ein AWS SDK verwenden oder HTTP-Anfragen direkt stellen.

Um eine Absenderauthentifizierungsrichtlinie zu löschen, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-identity-policy --identity example.com --policy-name samplePolicy
```

  Ersetzen Sie diesen Befehl *example.com* durch die Identität, die die Absenderauthentifizierungsrichtlinie enthält. *samplePolicy*Ersetzen Sie es durch den Namen der Absenderauthentifizierungsrichtlinie.

Löschen von auf Empfangsregeln bezogenen Daten

Wenn Sie mit Amazon SES eingehende E-Mails empfangen, können Sie Empfangsregeln erstellen, die für eine oder mehrere Identitäten (E-Mail-Adressen oder Domänen) gelten. Diese Regeln bestimmen, wie Amazon SES eingehende E-Mails verarbeitet, die an bestimmte Identitäten gesendet werden.

So löschen Sie eine Empfangsregel mithilfe der Amazon SES-Konsole

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie unter Email Receiving (E-Mail-Empfang) Rule Sets (Regelsätze) aus.
3. Wenn die Empfangsregel Teil des aktiven Regelsatzes ist, wählen Sie View Active Rule Set (Aktiven Regelsatz anzeigen). Wählen Sie andernfalls den Regelsatz mit der Empfangsregel aus, die Sie löschen möchten.
4. Wählen Sie in der Liste der Empfangsregeln die Regel aus, die Sie löschen möchten.
5. Wählen Sie im Menü Actions die Option Delete.
6. Wählen Sie im Bestätigungsdialogfeld die Option Delete (Löschen).

Empfangsregeln können auch mithilfe der Amazon SES-API gelöscht werden. Das folgende Verfahren verwendet die AWS Command Line Interface (AWS CLI), um mit der Amazon SES SES-API zu interagieren. Sie können auch mit der API interagieren, indem Sie ein AWS SDK verwenden oder HTTP-Anfragen direkt stellen.

Um eine Empfangsregel zu löschen, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws ses delete-receipt-rule --rule-set myRuleSet --rule-name myReceiptRule
  ```

  Ersetzen Sie diesen Befehl *myRuleSet* durch den Namen des Empfangsregelsatzes, der die Empfangsregel enthält. *myReceiptRule*Ersetzen Sie ihn durch den Namen der Empfangsregel, die Sie löschen möchten.

Löschen von auf IP-Adressfilter bezogenen Daten

Wenn Sie mit Amazon SES eingehende E-Mails empfangen, können Sie Filter erstellen, um von bestimmten IP-Adressen gesendete Nachrichten explizit zu akzeptieren oder zu blockieren.

So löschen Sie einen IP-Adressfilter mithilfe der Amazon SES-Konsole

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie unter Email Receiving (E-Mail-Empfang) IP Address Filters (IP-Adressfilter) aus.
3. Wählen Sie in der Liste der IP-Adressfilter den Filter aus, den Sie entfernen möchten. Klicken Sie dann auf Delete (Löschen).

IP-Adressfilter können auch mithilfe der Amazon SES-API gelöscht werden. Das folgende Verfahren verwendet die AWS Command Line Interface (AWS CLI), um mit der Amazon SES SES-API zu interagieren. Sie können auch mit der API interagieren, indem Sie ein AWS SDK verwenden oder HTTP-Anfragen direkt stellen.

Um einen IP-Adressfilter mit dem zu löschen AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws ses delete-receipt-filter --filter-name IPfilter
  ```

  Ersetzen Sie diesen Befehl *IPfilter* durch den Namen des IP-Adressfilters, den Sie löschen möchten.

Löschen von Daten in E-Mail-Vorlagen

Wenn Sie zum Senden von E-Mails E-Mail-Vorlagen verwenden, können diese Vorlagen abhängig davon, wie sie von Ihnen konfiguriert wurden, möglicherweise personenbezogene Daten enthalten. Beispielsweise könnten Sie der Vorlage eine E-Mail-Adresse hinzugefügt haben, an die sich Empfänger wenden können, um weitere Informationen zu erhalten.

E-Mail-Vorlagen können nur mithilfe der Amazon SES-API gelöscht werden.

Um eine E-Mail-Vorlage mit dem zu löschen AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws ses delete-template --template-name sampleTemplate
  ```

  Ersetzen Sie diesen Befehl *sampleTemplate* durch den Namen der E-Mail-Vorlage, die Sie löschen möchten.

Löschen von Daten in benutzerdefinierten Vorlagen zur E-Mail-Verifizierung

Wenn Sie zum Verifizieren neuer E-Mail-Adressen benutzerdefinierte Vorlagen verwenden, können diese Vorlagen abhängig davon, wie sie von Ihnen konfiguriert wurden, möglicherweise personenbezogene Daten enthalten. Beispielsweise könnten Sie der Vorlage zur E-Mail-Verifizierung eine E-Mail-Adresse hinzugefügt haben, an die sich Empfänger wenden können, um weitere Informationen zu erhalten.

Benutzerdefinierte Vorlagen zur E-Mail-Verifizierung können nur mithilfe der Amazon SES-API gelöscht werden.

Um eine benutzerdefinierte E-Mail-Vorlage für die Bestätigung zu löschen, verwenden Sie AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

  ```
  aws ses delete-custom-verification-email-template --template-
  name verificationEmailTemplate
  ```

  Ersetzen Sie diesen Befehl *verificationEmailTemplate* durch den Namen der benutzerdefinierten E-Mail-Vorlage für die Bestätigung, die Sie löschen möchten.

Löschen Sie alle persönlichen Daten, indem Sie Ihr AWS Konto schließen

Es ist auch möglich, alle personenbezogenen Daten, die in Amazon SES gespeichert sind, durch Schließen Ihres AWS -Kontos zu löschen. Durch diese Aktion werden jedoch auch alle anderen Daten — persönliche oder nicht personenbezogene — gelöscht, die Sie in jedem anderen Dienst gespeichert haben. AWS

Wenn Sie Ihr AWS Konto schließen, werden die Daten in Ihrem AWS Konto 90 Tage lang aufbewahrt. Nach Ablauf dieses Aufbewahrungszeitraums werden sie dauerhaft gelöscht. Dieser Vorgang kann nicht rückgängig gemacht werden.

Um Ihr AWS Konto zu schließen

Vollständige Anweisungen zur Schließung Ihres AWS Kontos finden Sie unter AWS Konto schließen.

Identity and Access Management in Amazon S3

Sie können AWS Identity and Access Management (IAM) mit Amazon Simple Email Service (Amazon SES) verwenden, um anzugeben, welche SES-API-Aktionen ein Benutzer, eine Gruppe oder eine

Rolle ausführen kann. (In diesem Thema bezeichnen wir diese Entitäten zusammen als Benutzer.) Sie können auch steuern, welche E-Mail-Adressen der Benutzer für die Adressen "From", Empfänger und "Return-Path" der E-Mails verwenden kann.

Sie können beispielsweise eine IAM-Richtlinie erstellen, die Benutzern in Ihrer Organisation ermöglicht, E-Mails zu senden, aber keine administrativen Aktionen, wie die Überprüfung von Sendestatistiken, durchzuführen. Ein weiteres Beispiel: Sie können eine Richtlinie schreiben, mit der ein Benutzer E-Mails über SES von Ihrem Konto senden kann, aber nur, wenn eine bestimmte "From"-Adresse verwendet wird.

Zur Verwendung von IAM definieren Sie eine IAM-Richtlinie, also ein Dokument, das explizit Berechtigungen definiert, und die Richtlinie einem Benutzer zuweist. Weitere Informationen zum Erstellen von IAM-Richtlinien finden Sie im IAM-Benutzerhandbuch. Abgesehen vom Anwenden der Einschränkungen, die Sie in Ihrer Richtlinie festlegen, gibt es keine Änderungen daran, wie Benutzer mit SES interagieren oder darin, wie SES Anfragen ausführt.

> **Note**
>
> - Befindet sich Ihr Konto in der SES-Sandbox, verhindern seine Einschränkungen die Implementierung einiger dieser Richtlinien – siehe Anfordern von Produktionszugriff..
> - Sie können auch mithilfe von Sendeautorisierungsrichtlinien den Zugriff auf SES steuern. Während IAM-Richtlinien regeln, welche Aufgaben einzelne Benutzer ausführen können, beschränken Sendeautorisierungsrichtlinien, wie individuell verifizierte Identitäten verwendet werden können. Darüber hinaus können nur Sendeautorisierungsrichtlinien kontenübergreifenden Zugriff gewähren. Weitere Informationen zur Sendeautorisierung finden Sie unter Verwenden der Sendeautorisierung mit Amazon SES.

Wenn Sie erfahren möchten, wie SES-SMTP-Anmeldeinformationen für einen bestehenden Benutzer generiert werden, lesen Sie unter Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen nach.

Erstellen von IAM-Richtlinien für den Zugriff auf SES

In diesem Abschnitt wird erklärt, wie Sie IAM-Richtlinien speziell mit SES verwenden können. Weitere allgemeine Informationen zum Erstellen von IAM-Richtlinien finden Sie im IAM-Benutzerhandbuch.

Es gibt drei Gründe, IAM ggf. mit SES zu verwenden:

- Um den E-Mail-Versand einzuschränken.

- Um die Adressen "From", Empfänger und "Return-Path" der E-Mails zu beschränken, die der Benutzer sendet.
- Um allgemeine Aspekte der API-Nutzung zu kontrollieren, z. B. den Zeitraum, in dem ein Benutzer das anrufen darf APIs , zu dessen Nutzung er berechtigt ist.

Beschränken der Aktion

Um zu steuern, welche SES-Aktionen ein Benutzer durchführen kann, verwenden Sie das `Action`-Element einer IAM-Richtlinie. Sie können das `Action`-Element auf eine beliebige SES-API-Aktion festlegen, indem Sie dem API-Namen die kleingeschriebene Zeichenfolge `ses:` voranstellen. Sie können beispielsweise `Action` auf `ses:SendEmail`, `ses:GetSendStatistics` oder `ses:*` festlegen (für alle Aktionen).

Geben Sie dann je nach `Action` das `Resource`-Element wie folgt an:

Falls das **`Action`** Element nur den Zugriff auf das Senden von E-Mails erlaubt APIs (d. h. **`ses:SendEmail`** und/oder**`ses:SendRawEmail`**):

- Um dem Benutzer das Senden von einer beliebigen Identität in Ihrer zu ermöglichen AWS-Konto, setzen `Resource` Sie ihn auf *
- Um die Identitäten einzuschränken, von denen aus ein Benutzer senden darf, legen Sie den `Resource` Wert auf die ARNs Identitäten fest, deren Verwendung Sie dem Benutzer gestatten.

Wenn das **`Action`** Element den Zugriff auf alle erlaubt: APIs

- Wenn Sie die Identitäten, von denen der Benutzer senden kann, nicht beschränken möchten, setzen Sie `Resource` auf *.
- Wenn Sie die Identitäten, von denen ein Benutzer senden darf, beschränken möchten, müssen Sie zwei Richtlinien (oder zwei Anweisungen innerhalb einer Richtlinie) erstellen:
  - Eins, das auf eine explizite Liste der erlaubten Elemente `Resource` gesetzt non-email-sending APIs und auf * gesetzt ist `Action`
  - Eine, die auf eine der E-Mails sendenden APIs (`ses:SendEmail`und/oder`ses:SendRawEmail`) und auf die ARN (s) der Identitäten `Resource` gesetzt ist, deren Verwendung Sie dem Benutzer gestatten. `Action`

Eine Liste der verfügbaren SES-Aktionen finden Sie in der Amazon Simple Email Service API Reference. Wenn der Benutzer die SMTP-Schnittstelle verwenden möchte, müssen Sie mindestens den Zugriff auf `ses:SendRawEmail` erlauben.

Beschränken von E-Mail-Adressen

Wenn Sie den Benutzer auf bestimmte E-Mail-Adressen beschränken möchten, können Sie einen `Condition`-Block verwenden. Im `Condition`-Block geben Sie Bedingungen mithilfe von Bedingungsschlüsseln an, wie im IAM-Benutzerhandbuch beschrieben. Durch die Nutzung von Bedingungsschlüsseln können Sie die folgenden E-Mail-Adressen steuern:

> **Note**
>
> Diese Bedingungsschlüssel für E-Mail-Adressen gelten nur für die in der folgenden APIs Tabelle aufgeführten.

Bedingungsschlüssel	Description	API
`ses:Recipients`	Beschränkt die Empfänger adressen, einschließlich der Adressen "To", "CC" und "BCC".	`SendEmail` , `SendRawEmail`
`ses:FromAddress`	Beschränkt die "From"-Adresse.	`SendEmail` , `SendRawEmail` , `SendBounce`
`ses:FromDisplayName`	Beschränkt die "From"-Adresse, die als Anzeigename verwendet wird.	`SendEmail` , `SendRawEmail`
`ses:FeedbackAddress`	Beschränkt die "Return-Path"-Adresse. Dies ist die Adresse, an die Unzustellbarkeitsn achrichten und Beschwerden an Sie anhand von Feedback-E-Mails weitergeleitet werden können. Weitere Informati	`SendEmail` , `SendRawEmail`

Bedingungsschlüssel	Description	API
	onen zum Weiterleiten von Feedback per E-Mail finden Sie unter Verwenden von Benachrichtigungen für den Amazon-SES-E-Mail-Empfang.	
`ses:MultiRegionEndpointId`	Ermöglicht es Ihnen zu steuern, welche Endpunkt-ID beim Senden von E-Mails verwendet wird	`SendEmail` , `SendBulkEmail`

Einschränken durch die SES-API-Version

Durch die Verwendung des `ses:ApiVersion`-Schlüssels in Bedingungen können Sie den Zugriff auf SES basierend auf der Version der SES API einschränken.

> **Note**
>
> Die SES-SMTP-Schnittstelle verwendet SES API Version 2 von `ses:SendRawEmail`.

Beschränken der allgemeinen API-Nutzung

Durch die Verwendung von AWS-weiten Schlüsseln in Bedingungen können Sie den Zugriff auf SES anhand von Aspekten wie Datum und Uhrzeit einschränken, auf die der Benutzer Zugriff APIs hat. SES implementiert nur die folgenden AWS-weiten Richtlinienschlüssel:

- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:UserAgent`

- `aws:VpcSourceIp`

Weitere Informationen zu diesen Schlüsseln finden Sie im IAM-Benutzerhandbuch.

Beispiel-IAM-Richtlinien für SES

In diesem Thema finden Sie Beispiele für Richtlinien, die einen Benutzerzugriff auf SES ermöglichen, jedoch nur unter bestimmten Bedingungen.

Richtlinienbeispiele in diesem Abschnitt:

- Berechtigen von Vollzugriff auf alle SES-Aktionen
- Zulassen des Zugriffs nur auf SES API Version 2
- Erlauben von Zugriff nur auf Aktionen für den E-Mail-Versand
- Beschränken des Sendezeitraums
- Beschränken der Empfängeradressen
- Beschränken der "From"-Adresse
- Beschränken des Anzeigenamens des E-Mail-Absenders
- Beschränken der Zieladresse des Unzustellbarkeits- und Beschwerde-Feedbacks

Berechtigen von Vollzugriff auf alle SES-Aktionen

Mit der folgenden Richtlinie können Benutzer jede beliebige SES-Aktion aufrufen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:*"
      ],
      "Resource":"*"
    }
  ]
}
```

Zulassen des Zugriffs nur auf SES API Version 2

Mit der folgenden Richtlinie können Benutzer nur die SES-Aktionen der API Version 2 aufrufen.

JSON

```
{
                    "Version":"2012-10-17",
                    "Statement":[
                        {
                            "Effect":"Allow",
                            "Action":[
                            "ses:*"
                            ],
                            "Resource":"*",
                            "Condition": {
                                "StringEquals" : {
                                "ses:ApiVersion" : "2"
                                }
                            }
                        }
                    ]
                }
```

Erlauben von Zugriff nur auf Aktionen für den E-Mail-Versand

Mit der folgenden Richtlinie kann ein Benutzer E-Mails mithilfe von SES senden, aber keine administrativen Aktionen durchführen, wie z. B. den Zugriff auf SES-Sendestatistiken.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
```

```
      "Resource":"*"
    }
  ]
}
```

Beschränken des Sendezeitraums

Die folgende Richtlinie erlaubt es einem Benutzer, SES APIs nur im September 2018 anzurufen, um E-Mails zu senden.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "DateGreaterThan":{
          "aws:CurrentTime":"2018-08-31T12:00Z"
        },
        "DateLessThan":{
          "aws:CurrentTime":"2018-10-01T12:00Z"
        }
      }
    }
  ]
}
```

Beschränken der Empfängeradressen

Die folgende Richtlinie erlaubt es einem Benutzer, SES-E-Mail-Versand anzurufen APIs, jedoch nur an Empfängeradressen in der Domain example.com (*StringLike*Groß- und Kleinschreibung wird beachtet).

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringLike":{
          "ses:Recipients":[
            "*@example.com"
          ]
        }
      }
    }
  ]
}
```

Beschränken der "From"-Adresse

Die folgende Richtlinie erlaubt es einem Benutzer, SES-E-Mail-Versand anzurufen APIs, jedoch nur, wenn die Absenderadresse marketing@example.com lautet.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
```

```
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"marketing@example.com"
        }
      }
    }
  ]
}
```

Die folgende Richtlinie erlaubt es einem Benutzer, die SendBounceAPI aufzurufen, jedoch nur, wenn die Absenderadresse bounce@example.com lautet.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendBounce"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"bounce@example.com"
        }
      }
    }
  ]
}
```

Beschränken des Anzeigenamens des E-Mail-Absenders

Die folgende Richtlinie erlaubt es einem Benutzer, SES-E-Mail-Versand anzurufen APIs, jedoch nur, wenn der Anzeigename der Absenderadresse Marketing enthält (Groß- und Kleinschreibung *`StringLike`* wird beachtet).

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringLike":{
          "ses:FromDisplayName":"Marketing"
        }
      }
    }
  ]
}
```

Beschränken der Zieladresse des Unzustellbarkeits- und Beschwerde-Feedbacks

Die folgende Richtlinie erlaubt es einem Benutzer, SES-E-Mail-Versand anzurufen APIs, allerdings nur, wenn der „Return-Pfad“ der E-Mail auf feedback@example.com gesetzt ist.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
```

```
          "ses:FeedbackAddress":"feedback@example.com"
        }
      }
    }
  ]
}
```

AWS verwaltete Richtlinien für Amazon Simple Email Service

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS verwaltete Richtlinie: Amazon SESFull Access

Sie können die `AmazonSESFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Bietet Vollzugriff auf Amazon SES.

Die Berechtigungen für diese Richtlinie finden Sie unter Amazon SESFull Access in der Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: Amazon SESRead OnlyAccess

Sie können die `AmazonSESReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Bietet schreibgeschützten Zugriff auf Amazon SES.

Die Berechtigungen für diese Richtlinie finden Sie unter Amazon SESRead OnlyAccess in der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: Amazon SESService RolePolicy

Sie können die `AmazonSESServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Amazon SES ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Servicebezogene Rollenberechtigungen für Amazon SES.

Die Berechtigungen für diese Richtlinie finden Sie unter Amazon SESService RolePolicy in der Referenz zu AWS verwalteten Richtlinien.

Amazon Simple Email Service aktualisiert AWS verwaltete Richtlinien

Sehen Sie sich Details und Aktualisierungen der AWS verwalteten Richtlinien für Amazon Simple Email Service an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen.

Änderungen	Beschreibung	Date
Amazon Simple Email Service hat eine neue verwaltete Richtlinie hinzugefügt	Amazon Simple Email Service wurde `AmazonSESServiceRolePolicy` zur serviceverknüpften Rolle hinzugefügt`AWSServiceRoleForAmazonSES` , sodass SES Aktionen in Ihrem Namen ausführen kann	13. Mai 2024
Amazon Simple Email Service hat eine Richtliniendefinition aktualisiert	Amazon Simple Email Service hat den vorherigen Eintrag in dieser Tabelle (Zeile	30. April 2024

Änderungen	Beschreibung	Date
	unten) wie folgt klargeste llt: Amazon Simple Email Service wurde `ses:BatchGetMetricData` zur von Amazon SESRead OnlyAccess verwalteten Richtlinie hinzugefügt — dadurch wird Zugriff auf die SES-API gewährt BatchGetMetricData	
Amazon Simple Email Service hat eine Richtliniendefinition aktualisiert	Amazon Simple Email Service wurde `ses:BatchGet*` zur von Amazon SESRead OnlyAccess verwalteten Richtlinie hinzugefügt — dies ermöglicht den Zugriff auf die SES-API BatchGetMetricData	16. Februar 2024
Amazon Simple Email Service hat zwei Richtliniendefinitionen verändert	Amazon Simple Email Service hat „über die AWS Management Console“ vom Ende der Amazon SESFull Access- und SESRead OnlyAccess Amazon-De finitionen entfernt	3. Mai 2023
Amazon Simple Email Service hat mit der Änderungs verfolgung begonnen	Amazon Simple Email Service hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen	5. April 2023

Verwenden von serviceverknüpften Rollen für Amazon SES

Amazon Simple Email Service (SES) verwendet AWS Identity and Access Management (IAM) service-verknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon SES verknüpft ist. Servicebezogene Rollen sind von SES vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von SES, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. SES definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur SES seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre SES-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entziehen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Dienstverknüpfte Rollen nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Servicebezogene Rollenberechtigungen für Amazon SES

SES verwendet die serviceverknüpfte Rolle AWSServiceRoleForAmazonSES — Ermöglicht SES, CloudWatch grundlegende Überwachungsmetriken von Amazon im Namen Ihrer SES-Ressourcen zu veröffentlichen.

Die serviceverknüpfte AWSService RoleForAmazon SES-Rolle vertraut darauf, dass der folgende Service die Rolle übernimmt:

- `ses.amazonaws.com`

Die Rollenberechtigungsrichtlinie mit dem Namen Amazon SESService RolePolicy ist eine AWS verwaltete Richtlinie, die es SES ermöglicht, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `cloudwatch:PutMetricData` im `AWS/SES` CloudWatch Namespace. Diese Aktion erteilt SES die Erlaubnis, Metrikdaten in den CloudWatch `AWS/SES` Namespace zu stellen. Weitere

Informationen zu SES-Metriken, die in verfügbar sind CloudWatch, finden Sie unterProtokollierung und Überwachung in Amazon SES.

- Aktion: `cloudwatch:PutMetricData` im `AWS/SES/MailManager` CloudWatch Namespace. Diese Aktion erteilt SES die Erlaubnis, Metrikdaten in den CloudWatch `AWS/SES/MailManager` Namespace zu stellen. Weitere Informationen zu SES-Metriken, die in verfügbar sind CloudWatch, finden Sie unterProtokollierung und Überwachung in Amazon SES.
- Aktion: `cloudwatch:PutMetricData` im `AWS/SES/Addons` CloudWatch Namespace. Diese Aktion erteilt SES die Erlaubnis, Metrikdaten in den CloudWatch `AWS/SES/Addons` Namespace zu stellen. Weitere Informationen zu SES-Metriken, die in verfügbar sind CloudWatch, finden Sie unterProtokollierung und Überwachung in Amazon SES.

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Amazon SES erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie SES-Ressourcen in der AWS-Managementkonsole, der oder der AWS API erstellen AWS CLI, erstellt SES die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie SES-Ressourcen erstellen, erstellt SES die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Amazon SES

SES erlaubt Ihnen nicht, die serviceverknüpfte AWSService RoleForAmazon SES-Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten.

Löschen einer serviceverknüpften Rolle für SES

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer dienstbezogenen Rolle

Bevor Sie IAM verwenden können, um eine dienstverknüpfte Rolle zu löschen, müssen Sie zunächst alle SES-Ressourcen löschen.

> **Note**
>
> Wenn der SES-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die mit dem AWSService RoleForAmazon SES-Dienst verknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für Rollen im Zusammenhang mit dem Service von Amazon SES

SES unterstützt die Verwendung von servicebezogenen Rollen nicht in allen Regionen, in denen der Service verfügbar ist. Sie können die AWSService RoleForAmazon SES-Rolle in den folgenden Regionen verwenden.

Name der Region	Regions-ID	Support in SES
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Ireland)	eu-west-1	Ja

Protokollierung und Überwachung in Amazon SES

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon SES und Ihrer AWS Lösungen. AWS bietet Tools, mit denen Sie Amazon SES überwachen und auf potenzielle Vorfälle reagieren können.

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Weitere Informationen erhalten Sie unter Amazon SES SES-Ereignisdaten werden abgerufen von CloudWatch und Erstellen von Alarmen zur Reputationsüberwachung mit CloudWatch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie unter Protokollieren Amazon SES SES-API-Aufrufen mit AWS CloudTrail.
- Amazon SESE-Mail-Sendeereignissenkann Ihnen bei der Feinabstimmung Ihrer E-Mail-Versandstrategie helfen. Amazon SES erfasst detaillierte Informationen, einschließlich der gesendeten, angeklickten, angeklickten, unzustellbaren und abgelehnten E-Mails sowie Beschwerden. Weitere Informationen finden Sie unter Überwachen der SMS-Aktivität.
- Amazon SESMetriken für die Zuverlässigkeitverfolgt die Unzustellbaren und Beschwerderaten für Ihr Konto. Weitere Informationen finden Sie unter Überwachen Ihrer Absenderzuverlässigkeit.

Protokollieren Amazon SES SES-API-Aufrufen mit AWS CloudTrail

Amazon SES ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in SES ausgeführt wurden. CloudTrail erfasst API-Aufrufe für SES als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der SES-Konsole und Codeaufrufen für die SES-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für SES. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an SES gestellt wurde,

die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen darüber CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrail Benutzerhandbuch.

SES-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in SES auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für SES, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

SES-Datenereignisse in CloudTrail

Datenereignisse liefern Informationen über die Ressourcenoperationen, die an oder in einer Ressource ausgeführt werden. Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume. Protokolliert standardmäßig CloudTrail keine Datenereignisse. Der CloudTrail Ereignisverlauf zeichnet keine Datenereignisse auf.

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preisgestaltung.

> **Note**
>
> Der Versand von E-Mails über die SMTP-Schnittstelle von SES wird nicht in den CloudTrail Ereignissen protokolliert. Für eine umfassende Protokollierung von Aktivitäten verwenden Sie die neuesten SES-Versionen APIs in der SES-API-Referenz und der SES-API-v2-Referenz.

In der folgenden Tabelle sind die SES-Ressourcentypen aufgeführt, für die Sie Datenereignisse protokollieren können. In der Spalte Datenereignistyp (Konsole) wird der Wert angezeigt, den Sie in der Liste Datenereignistyp auf der CloudTrail Konsole auswählen können. In der Wertspalte resources.type wird der `resources.type` Wert angezeigt, den Sie bei der Konfiguration erweiterter Event-Selektoren mithilfe der Spalte mit dem Symbol oder angeben würden. AWS CLI CloudTrail APIs In der CloudTrail Spalte APIs Protokollierte Daten werden die API-Aufrufe angezeigt, die CloudTrail für den Ressourcentyp protokolliert wurden.

SES-Ressourcentypen für Datenereignisse

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten APIs wurden protokolliert CloudTrail
SES-Identität	AWS: :SES:: EmailIdentity	SES:
SES-Konfigurationssatz	AWS: :SES:: ConfigurationSet	SendEmail SendRawEmail SendTemplatedEmail SendBulkTemplatedEmail

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten APIs wurden protokolliert CloudTrail
		SES v2: SendEmail SendBulkEmail
SES-Vorlage	AWS: :SES: :Vorlage	SES: SendTemplatedEmail SendBulkTemplatedEmail SES v2: SendEmail SendBulkEmail

Das folgende Beispiel zeigt, wie alle Datenereignisse für alle SES-E-Mail-Identitäten mithilfe des `--advanced-event-selectors` Parameters protokolliert werden:

```
aws cloudtrail put-event-selectors \
--region Region \
--trail-name TrailName \
--advanced-event-selectors
'[
    {
        "Name": "Log SES data plane actions for all email identities",
        "FieldSelectors": [
        { "Field": "eventCategory", "Equals": ["Data"] },
        { "Field": "resources.type", "Equals": ["AWS::SES::EmailIdentity"] }
       ]
    }
]'
```

Sie können die erweiterten Ereignisauswahlen weiter verfeinern, um nach den `resources.ARN` Feldern, und zu filtern `eventNamereadOnly`, sodass nur die Ereignisse protokolliert werden, die für Sie wichtig sind. Weitere Informationen zu diesen Kontingenten finden Sie unter

AdvancedFieldSelector in derAWS CloudTrail -API-Referenz. Weitere Beispiele zum Protokollieren von Datenereignissen finden Sie unter Datenereignisse für Trails protokollieren.

CloudTrail Szenarien zur Protokollzustellung für die SES-Protokollierung

CloudTrail liefert Protokolle, die auf Faktoren wie Konto- und Ressourcenbesitz, Identitätstyp und Region basieren. In der folgenden Matrix wird anhand bestimmter Kombinationen dieser Faktoren erklärt, an wen und an wen die Protokolle gesendet werden sollen.

Art des Szenarios	Kontorollen	Ressourcen	Ablauf der Anfrage	Protokoll zustellung
Ein einziges Konto für mehrere Konten	Konto A: Besitzer der Ressource Konto B: Anforderer	E-Mail-Identität	B → E-Mail-Id entität von A	Protokolle, die sowohl an A als auch an B gesendet wurden
		E-Mail zur Weiterleitung von Feedback	B → Feedback-E-Mail von A	Protokolle, die sowohl an A als auch an B gesendet wurden
Mehrere kontoüber greifende Konten	Konto A: Inhaber der Feedback-E-Mail Konto B: Inhaber der E-Mail-Id entität Konto C: Anforderer	Feedback-E-Mail (A) E-Mail-Identität (B)	C → Feedback-E-Mail von A + E-Mail-Identität von B	An A, B und C gelieferte Protokolle
Globaler Endpunkt (Einzelkonto)	Konto A: Eigentümer und Anforderer	Globaler Endpunkt (primär: eu-west-1 und sekundär: us-west-2)	A → Globaler Endpunkt	Protokolle, die an A in der Region übermitte lt wurden, in der die Anfrage bearbeitet

Art des Szenarios	Kontorollen	Ressourcen	Ablauf der Anfrage	Protokoll zustellung
				wurde (entweder EU-West-1 oder US-West-2)
Globaler Endpunkt (kontoübergreifend)	Konto A: Inhaber der E-Mail-Id entität Konto B: Anforderer	E-Mail-Identität (A) Globaler Endpunkt (B) (eu-west-1 und us-west-2)	B → E-Mail-Id entität von A über globalen Endpunkt	Protokolle, die sowohl an A als auch an B in der Region gesendet wurden, in der die Anfrage bearbeitet wurde (entweder EU-West-1 oder US-West-2)

Note

- CloudTrail übermittelt die Protokolle immer an das Konto des Anfragenden.
- Ressourcenbesitzer erhalten Protokolle, auch wenn sie den Vorgang nicht ausgeführt haben.
- Für globale Endgeräte benötigen beide Konten CloudTrail Abonnements in allen konfigurierten Regionen.
- Bei regionalen Einschränkungen werden alle Protokolle in der fehlerfreien Region angezeigt.

SES-Managementereignisse in CloudTrail

SES führt Managementereignisse für durch CloudTrail. Managementereignisse umfassen Aktionen, die sich auf die Erstellung und Verwaltung von Ressourcen innerhalb Ihres Unternehmens beziehen AWS-Konto. In Amazon SES umfassen Verwaltungsereignisse Aktionen, wie z. B. Erstellen und Löschen von Identitäten oder Empfangsregeln. Weitere Informationen zu SES-API-Vorgängen finden Sie in der SES-API-Referenz und der SES-API-v2-Referenz.

CloudTrail Protokolldateieinträge für SES

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Die folgenden Beispiele veranschaulichen CloudTrail Protokolle dieser Ereignistypen:

Ereignistypen

- DeleteIdentity
- VerifyEmailIdentity
- SendEmail mit einfachem Inhalt
- SendEmail mit Inhalten mit Vorlagen

DeleteIdentity


```
{
  "Records":[
    {
        "eventVersion": "1.11",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROA4DO2KAWIPZEXAMPLE:myUserName",
            "arn": "arn:aws:sts::111122223333:assumed-role/users/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AROA4DO2KAWIPZEXAMPLE",
                    "arn": "arn:aws:iam::111122223333:role/admin-role",
                    "accountId": "111122223333",
                    "userName": "myUserName"
                },
                "attributes": {
                    "creationDate": "2025-02-27T09:53:35Z",
                    "mfaAuthenticated": "false"
```

```
                }
            }
        },
        "eventTime": "2025-02-27T09:54:31Z",
        "eventSource": "ses.amazonaws.com",
        "eventName": "DeleteIdentity",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "aws-cli/2.23.4",
        "requestParameters": {
            "identity": "sender@example.com"
        },
        "responseElements": null,
        "requestID": "50b87bfe-ab23-11e4-9106-5b36376f9d12",
        "eventID": "0ffa308d-1467-4259-8be3-c749753be325",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management",
        "tlsDetails": {
            "tlsVersion": "TLSv1.3",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
            "clientProvidedHostHeader": "email.us-east-1.amazonaws.com"
        }
    }
  ]
}
```

VerifyEmailIdentity

```
{
  "Records":[
    {
        "eventVersion": "1.11",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROA4DO2KAWIPZEXAMPLE:myUserName",
            "arn": "arn:aws:sts::111122223333:assumed-role/users/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
```

```
                    "type": "Role",
                    "principalId": "AROA4DO2KAWIPZEXAMPLE",
                    "arn": "arn:aws:iam::111122223333:role/admin-role",
                    "accountId": "111122223333",
                    "userName": "myUserName"
                },
                "attributes": {
                    "creationDate": "2025-02-27T09:53:35Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2025-02-27T09:56:20Z",
        "eventSource": "ses.amazonaws.com",
        "eventName": "VerifyEmailIdentity",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "aws-cli/2.23.4",
        "requestParameters": {
            "emailAddress": "sender@example.com"
        },
        "responseElements": null,
        "requestID": "eb2ff803-ac09-11e4-8ff5-a56a3119e253",
        "eventID": "5613b0ff-d6c6-4526-9b53-a603a9231725",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management",
        "tlsDetails": {
            "tlsVersion": "TLSv1.3",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
            "clientProvidedHostHeader": "email.us-east-1.amazonaws.com"
        }
    }
  ]
}
```


SendEmail mit einfachem Inhalt


```
{
  "Records":[{
       "eventTime": "2025-01-24T11:43:00Z",
```

```
        "eventSource": "ses.amazonaws.com",
        "eventName": "SendEmail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "aws-cli/2.23.4 md/awscrt#0.23.4",
        "requestParameters": {
            "destination": {
                "bccAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
                "toAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
                "ccAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"]
            },
            "message": {
                "subject": {
                    "charset": "UTF-8",
                    "data": "HIDDEN_DUE_TO_SECURITY_REASONS"
                },
                "body": {
                    "html": {
                        "charset": "UTF-8",
                        "data": "HIDDEN_DUE_TO_SECURITY_REASONS"
                    },
                    "text": {
                        "charset": "UTF-8",
                        "data": "HIDDEN_DUE_TO_SECURITY_REASONS"
                    }
                }
            },
            "source": "sender@example.com"
        },
        "responseElements": null,
        "additionalEventData": {
            "sesMessageId": "01000100a11a11aa-00aa0a00-00a0-48a8-aaa7-
a174a83b456a-000000"
        },
        "requestID": "ab2cc803-ac09-11d7-8bb8-a56a3119e476",
        "eventID": "eb834e01-f168-435f-92c0-c36278378b6e",
        "readOnly": true,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::SES::EmailIdentity",
            "ARN": "arn:aws:ses:us-east-1:111122223333:identity/sender@example.com"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
```

```
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.3",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
            "clientProvidedHostHeader": "email.us-east-1.amazonaws.com"
        }
    }
  ]
}
```

SendEmail mit Inhalten mit Vorlagen

```
{
        "eventVersion": "1.11",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "AROA4DO2KAWIPZEXAMPLE:myUserName",
            "arn": "arn:aws:sts::111122223333:assumed-role/users/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AROA4DO2KAWIPZEXAMPLE",
                    "arn": "arn:aws:iam::111122223333:role/admin-role",
                    "accountId": "111122223333",
                    "userName": "admin-role"
                },
                "attributes": {
                    "creationDate": "2025-03-05T18:51:06Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2025-03-05T19:16:29Z",
        "eventSource": "ses.amazonaws.com",
        "eventName": "SendEmail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "aws-cli/2.23.4",
        "requestParameters": {
            "fromEmailAddress": "sender@example.com",
```

```
            "destination": {
                "toAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
                "bccAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
                "ccAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"]
            },
            "emailTags": [{
                "value": "test",
                "name": "campaign"
            }, {
                "value": "cli-test",
                "name": "sender"
            }],
            "replyToAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
            "content": {
                "template": {
                    "templateData": "HIDDEN_DUE_TO_SECURITY_REASONS",
                    "templateName": "TestTemplate"
                }
            }
        },
        "responseElements": null,
        "additionalEventData": {
            "sesMessageId": "01000100a11a11aa-00aa0a00-00a0-48a8-aaa7-
a174a83b456a-000000"
        },
        "requestID": "50b87bfe-ab23-11e4-9106-5b36376f9d12",
        "eventID": "0ffa308d-1467-4259-8be3-c749753be325",
        "readOnly": true,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::SES::EmailIdentity",
            "ARN": "arn:aws:ses:us-east-1:111122223333:identity/sender@example.com"
        }, {
            "accountId": "111122223333",
            "type": "AWS::SES::Template",
            "ARN": "arn:aws:ses:us-east-1:111122223333:template/TestTemplate"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.3",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
```

```
            "clientProvidedHostHeader": "email.us-east-1.amazonaws.com"
        }
    }
```

Compliance-Validierung für Amazon Simple Email Service

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon Simple Email Service im Rahmen mehrerer AWS Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS . Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung in Bezug auf die Compliance bei der Verwendung von -Services ergibt sich aus der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens sowie den einschlägigen Gesetzen und Vorschriften. AWS stellt die folgenden Ressourcen zur Sicherstellung der Compliance bereit:

- Schnellstartanleitungen zu Sicherheit und Compliance Schnellstartanleitungen zu — In diesen Bereitstellungshandbüchern werden architektonische Überlegungen erörtert und Schritte für die Implementierung von sicherheits- und Compliance-orientierten Basisumgebungen beschrieben. AWS
- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Bewertung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — AWS Config; bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub CSPM— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen können AWS , ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.

Amazon Simple Email Service

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur in Amazon OpenSearch Service

Als verwalteter Service ist Amazon Simple Email Service durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon Simple Email Service zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Einrichten von VPC-Endpunkten mit Amazon SES

Viele Amazon SES-Kunden verfügen über Unternehmensrichtlinien, die die Fähigkeit ihrer internen Systeme, sich mit dem öffentlichen Internet zu verbinden, einschränken. Diese Richtlinien verhindern, dass die öffentlichen Amazon-SES-Endpunkte verwendet werden.

Wenn Sie über ähnliche Richtlinien verfügen, können Sie innerhalb dieser Einschränkungen arbeiten, indem Sie Amazon Virtual Private Cloud verwenden. Mit Amazon VPC können Sie AWS Ressourcen

in einem virtuellen Netzwerk bereitstellen, das sich in einem isolierten Bereich des AWS Cloud befindet. Weitere Informationen zur Amazon VPC-Sicherheit finden Sie unter Sicherheit im Amazon VPC-Benutzerhandbuch.

Sie können über einen VPC-Endpunkt auf sichere und skalierbare Weise direkt von Amazon VPC eine Verbindung mit SES herstellen. Wenn Sie einen Schnittstellen-VPC-Endpunkt verwenden, wird eine bessere Sicherheitslage ermöglicht, da Sie keine Firewalls für ausgehenden Datenverkehr öffnen müssen. Außerdem ergeben sich weitere Vorteile aus der Verwendung von Amazon-VPC-Endpunkten.

Wenn Sie einen VPC-Endpunkt verwenden, wird der Datenverkehr an SES nicht über das Internet übertragen und verlässt niemals das Amazon-Netzwerk, um Ihre VPC ohne Verfügbarkeitsrisiken oder Bandbreitenbeschränkungen für Ihren Netzwerkverkehr sicher mit SES zu verbinden. Sie können SES in Ihrer Infrastruktur mit mehreren Konten zentralisieren und es als Service für Ihre Konten bereitstellen, ohne ein Internet-Gateway verwenden zu müssen.

Einschränkungen

- SES unterstützt keine SMTP-VPC-Endpunkte in den folgenden Availability Zones:`use1-az2`,`use1-az3`,`use1-az5`,, `usw1-az2` `usw2-az4`apne2-az4, `cac1-az3` und. `cac1-az4`
- Der SMTP-Endpunkt, der in der VPC verwendet wird, ist auf die AWS-Region beschränkt, die aktuell für Ihr Konto verwendet wird.

Sie können VPC-Endpunkte auch mit Mail Manager-Eingangsendpunkten für eine sichere, private E-Mail-Aufnahme innerhalb Ihrer privaten Netzwerkinfrastruktur verwenden. Weitere Informationen finden Sie im Kapitel Mail Managerthe section called “VPC-Endpunktkonfiguration”.

Anleitungsbeispiel für die Einrichtung von SES in Amazon VPC

Voraussetzungen

Bevor Sie das Verfahren in diesem Abschnitt ausführen, müssen Sie die folgenden Schritte ausführen:

- Sie benötigen eine vorhandene Virtual Private Cloud (VPC) oder müssen eine neue VPC erstellen. Weitere Informationen finden Sie unter Erste Schritte mit Amazon VPC.

- Starten Sie eine Amazon-EC2-Instance in Ihrer VPC, um die Verbindung mit dem VPC-Endpunkt zu testen, der in einem späteren Schritt erstellt wird. Weitere Informationen finden Sie unter Standard VPCs.

> **Note**
>
> VPC-Endpunkte für SES können zwar mit jeder Ressource verwendet werden, zur Vereinfachung der Testmethode verwenden Sie in diesem Beispiel jedoch eine EC2-Instance als Ressource. Da Amazon EC2 den E-Mail-Verkehr über Port 25 standardmäßig einschränkt, müssen Sie für SMTP-Endpunkte einen anderen Port als TCP 25 verwenden, z. B. TCP 465, 587, 2465 oder 2587. Weitere Informationen finden Sie unter Beschränkung für E-Mails, die über Port 25 gesendet werden. Verwenden Sie für API-Endpunkte Port 443.

Einrichten von SES in Amazon VPC

Der Vorgang zum Einrichten eines VPC-Endpunkts zur Verwendung mit SES besteht aus wenigen separaten Schritten. Zunächst müssen Sie eine Sicherheitsgruppe erstellen, die es der Instance ermöglicht, mit den ausgewählten Ports zu kommunizieren, dann einen VPC-Endpunkt für Amazon SES erstellen und schließlich die Verbindung zum VPC-Endpunkt testen, um sicherzustellen, dass sie ordnungsgemäß konfiguriert ist.

Schritt 1: Erstellen der Sicherheitsgruppe

In diesem Schritt erstellen Sie eine Sicherheitsgruppe, die die Amazon-EC2-Instances mit dem VPC-Schnittstellenendpunkt kommunizieren lässt, den Sie erstellen werden.

So erstellen Sie die Sicherheitsgruppe

1. Wählen Sie im Navigationsbereich der Amazon EC2-Konsole unter Network & Security (Netzwerk und Sicherheit) die Option Security Groups (Sicherheitsgruppen) aus.
2. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
3. Gehen Sie unter Basic details (Grundlegende Angaben) wie folgt vor:
   - Geben Sie unter Security group name (Name der Sicherheitsgruppe) einen eindeutigen Namen ein, der die Sicherheitsgruppe identifiziert.
   - Geben Sie für Description (Beschreibung) einen Text ein, der den Zweck der Sicherheitsgruppe beschreibt.

- Wählen Sie unter VPC die VPC aus, in der Sie Amazon SES verwenden möchten.

4. Wählen Sie unter Inbound rules (Regeln für eingehenden Datenverkehr) die Option Add rule (Regel hinzufügen).
5. Für die neue Eingehende Regel gehen Sie folgendermaßen vor:

   - Wählen Sie für Type (Typ) die Option Custom TCP (Benutzerdefiniertes TCP) aus.
   - Geben Sie unter Port range (Portbereich) die Portnummer ein, die Sie für den E-Mail-Versand verwenden möchten. Für SMTP-Endpunkte können Sie eine der folgenden Portnummern verwenden:**465**,, **587** oder. **2465 2587** Verwenden Sie für API-Endpunkte Port 443.
   - Wählen Sie für den Source type (Quelltyp) die Option Custom (Benutzerdefiniert).
   - Geben Sie als Quelle den privaten IP-CIDR-Bereich oder eine andere Sicherheitsgruppe ein IDs , die die Ressourcen enthält, die den VPC-Endpunkt für die Kommunikation mit dem SES-Dienst verwenden.
   - (Wiederholen Sie die Schritte 4 bis 5 für jeden CIDR-Bereich oder jede Sicherheitsgruppe, von dem bzw. der aus Sie Zugriff gewähren möchten.)
6. Wenn Sie fertig sind, wählen Sie Sicherheitsgruppe erstellen aus.

Schritt 2: Erstellen des VPC-Endpunkts

In Amazon VPC können Sie mit einem VPC-Endpunkt Ihre VPC mit unterstützten Services verbinden. AWS In diesem Beispiel konfigurieren Sie Amazon VPC so, dass Ihre Amazon-EC2-Sicherheitsgruppe eine Verbindung mit Amazon SES herstellen kann.

Erstellen des VPC-Endpunkts

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie unter PrivateLink und Lattice die Option Endpoints aus.
3. Klicken Sie auf Create Endpoint (Endpunkt erstellen), um die Seite Create Endpoint (Endpunkt erstellen) zu öffnen.
4. (Optional) Erstellen Sie im Bereich Endpoint settings (Endpunkt-Einstellungen) ein Tag im Feld Name tag (Tag benennen).
5. Wählen Sie als Service category (Servicekategorie) die Option AWS services (AWS -Services) aus.
6. Filtern Sie im Bereich Dienste für SMTP-Endpunkte in der Suchleiste nach SMTP und wählen Sie dann das entsprechende Optionsfeld aus. Filtern Sie bei API-Endpunkten in der Suchleiste

nach E-Mails. Sie können auch einen FIPS-Endpunkt verwenden, indem Sie nach E-Mail-FIPS suchen.

7. Klicken Sie im Bereich VPC in die Suchleiste und wählen Sie eine VPC aus dem Listenfeld aus (siehe the section called “Voraussetzungen”).
8. Wählen Sie im Bereich Subnetze die Optionen Availability Zones und Subnet aus. IDs

   > **Note**
   >
   > Amazon SES unterstützt keine SMTP-VPC-Endpunkte in den folgenden Availability Zones:`use1-az2`,`use1-az3`,`use1-az5`,, `usw1-az2` `usw2-az4`apne2-az4, `cac1-az3` und. `cac1-az4`

9. Wählen Sie im Bereich Security Groups (Sicherheitsgruppen) die Sicherheitsgruppe aus, die Sie zuvor erstellt haben.
10. (Optional) Im Bereich Tags können Sie ein oder mehrere Tags erstellen.
11. Wählen Sie Create endpoint (Endpunkt erstellen). Warten Sie etwa 5 Minuten, während Amazon VPC den Endpunkt erstellt. Wenn der Endpunkt einsatzbereit ist, ändert sich der Wert in der Spalte Status auf Status auf Available (Verfügbar).

(Optional) Schritt 3: Testen der Verbindung mit dem VPC-Endpunkt

Wenn Sie die Konfiguration des VPC-Endpunkts abgeschlossen haben, können Sie die Verbindung testen, um sicherzustellen, dass der VPC-Endpunkt korrekt konfiguriert ist. Sie können die Verbindung testen, indem Sie Befehlszeilen-Tools verwenden, die mit den meisten Betriebssystemen mitgeliefert werden.

So testen Sie die Verbindung zum VPC-Endpunkt

1. Starten Sie eine Amazon-EC2-Instance in derselben VPC, in der Sie gerade den VPC-Endpunkt „email-smtp“ erstellt haben.

   Informationen zum Herstellen einer Verbindung zu Linux-Instances finden Sie unter Connect to your Linux Instance im Amazon EC2 EC2-Benutzerhandbuch.

   Informationen zum Herstellen einer Verbindung zu Windows-Instances finden Sie im Tutorial Erste Schritte im Amazon EC2 EC2-Benutzerhandbuch.

2. Senden einer Test-E-Mail Verwenden Sie für den SMTP-Endpunkt die SES SMTP-Schnittstelle. Verwenden Sie für den API-Endpunkt die SES-CLI oder API.

> **Note**
>
> Sie müssen eine E-Mail-Adresse oder Domain verifizieren, bevor Sie E-Mails über Amazon SES versenden können. Weitere Informationen zur Überprüfung von Identitäten finden Sie unter Erstellen und verifizieren von Identitäten in Amazon SES.

Fehlersuche bei Amazon SES

Dieser Abschnitt enthält die folgenden Themen, die Ihnen bei Problemen helfen können:

- Informationen zu möglichen Problemen im Zusammenhang mit der Domänenverifizierung finden Sie unter Probleme bei der Verifizierung von Domänen und E-Mail-Adressen.
- Lösungen für Probleme im Zusammenhang mit DKIM finden Sie unter Beheben von DKIM-Problemen in Amazon SES.
- Eine Liste häufiger Zustellungsprobleme, die auftreten können, wenn Sie E-Mails versenden, sowie Abhilfemaßnahmen, die Sie ausführen können, finden Sie unter Amazon SES-Zustellungsprobleme.
- Eine Beschreibung der Probleme, die Empfängern möglicherweise angezeigt werden, wenn sie eine E-Mail erhalten, die über Amazon SES gesendet wurde, finden Sie unter Probleme mit E-Mails von Amazon SES.
- Lösungen für Probleme mit Unzustellbarkeits-, Beschwerde- und Zustellungsbenachrichtigungen finden Sie unter Probleme mit Amazon SES-Benachrichtigungen.
- Eine Liste der Fehler, die auftreten können, wenn Sie eine E-Mail mit Amazon SES senden, finden Sie unter Fehler beim Senden von E-Mails über Amazon SES.
- Tipps zur Beschleunigung des E-Mail-Versands bei mehreren Aufrufen von Amazon SES über die API oder die SMTP-Schnittstelle finden Sie unter Erhöhen des Durchsatzes mit Amazon SES.
- Lösungen für häufige Probleme, die auftreten können, wenn Sie Amazon SES über die SMTP-Schnittstelle (Simple Mail Transfer Protocol) verwenden, sowie eine Liste der von Amazon SES zurückgegebenen SMTP-Antwortcodes finden Sie unter SMTP-Probleme bei Amazon SES.
- Eine Liste der häufigsten Fehlercodes, die von der Amazon SES API-v2 zurückgegeben werden, finden Sie unter.Häufige Fehleraus.
- Eine Beschreibung häufiger Probleme im Zusammenhang mit unserer Sendeprüfung und deren Behandlung finden Sie unter Amazon SES Versandprüfungsprozess FAQs.
- Eine Erläuterung darüber, wie sich DNS-basierte Blackhole Lists (DNSBLs) auf Ihren Versand mit Amazon SES auswirken, finden Sie unter. DNS-Blackhole-Liste (DNSBL) FAQs

Informationen darüber, wie Sie Amazon SES API direkt aufrufen, finden Sie unterAmazon Simple Email Service API-Referenzfür die HTTP-Fehler, die Sie möglicherweise erhalten,.

> **Note**
>
> Wenn Sie technischen Support benötigen, verwenden Sie nicht den Feedback-Link auf einer der Seiten dieses Entwicklerhandbuchs, da das Formular vom AWS Dokumentationsteam und nicht vom AWS Support empfangen wird. Sehen Sie sich stattdessen auf der Seite Kontakt die verschiedenen verfügbaren Support-Optionen an.

Inhalt

- Allgemeine Amazon SES-Probleme
- Probleme bei der Verifizierung von Domänen und E-Mail-Adressen
- Beheben von DKIM-Problemen in Amazon SES
- Amazon SES-Zustellungsprobleme
- Probleme mit E-Mails von Amazon SES
- Probleme mit Amazon SES-Benachrichtigungen
- Fehler beim Senden von E-Mails über Amazon SES
- Erhöhen des Durchsatzes mit Amazon SES
- SMTP-Probleme bei Amazon SES

Allgemeine Amazon SES-Probleme

Die auf dieser Seite aufgeführten Informationen beschreiben Probleme, die bei der Verwendung von Amazon SES auftreten können, und helfen Ihnen, diese zu diagnostizieren.

Änderungen, die ich vornehme, sind nicht direkt sichtbar

Als Service, auf den Computer in weltweit angesiedelten Rechenzentren zugreifen, nutzt Amazon SES ein verteiltes Computing-Modell namens letztendliche Konsistenz. Jede Änderung, die Sie an Amazon SES (oder anderen AWS Services) vornehmen, dauert einige Zeit, bis sie von allen möglichen Endpunkten aus sichtbar wird. Die Verzögerung ergibt sich teilweise aus der Zeit, die erforderlich ist, um die Daten von Server zu Server und von einer Region der Welt in eine andere zu senden. In den meisten Fällen beträgt diese nicht mehr als ein paar Minuten.

Zu den Bereichen, in denen eine Verzögerung auftreten kann, gehören:

- Erstellen und Bearbeiten von Konfigurationssätzen – Wenn Sie einen Konfigurationssatz erstellen oder ändern (beispielsweise bei der Verknüpfung eines dedizierten IP-Pools mit einem vorhandenen Konfigurationssatz), kann eine kurze Verzögerung auftreten, und zwar zwischen dem Zeitpunkt der Erstellung oder Änderung und dem Zeitpunkt der Aktivierung dieser Änderungen.
- Event-Ziele erstellen und ändern — Wenn Sie ein Event-Ziel erstellen oder ändern (z. B. um Amazon SES anzuweisen, Ihre E-Mail-Sendedaten an einen anderen AWS Service zu senden), kann es zu einer Verzögerung zwischen dem Zeitpunkt, zu dem Sie das Event-Ziel erstellt oder geändert haben, und dem Zeitpunkt, zu dem E-Mail-Versandereignisse tatsächlich am angegebenen Ziel ankommen, zu einer Verzögerung kommen.

Probleme bei der Verifizierung von Domänen und E-Mail-Adressen

Verwenden Sie entweder die Amazon-SES-Konsole oder die Amazon-SES-API, um den Verifizierungsprozess für eine Domäne oder E-Mail-Adresse mit Amazon SES zu initiieren. Dieser Abschnitt enthält Informationen, die helfen können, Probleme mit der Verifizierung zu lösen.

> **Note**
>
> In den folgenden Verfahren könnte sich der Verweis auf DNS-Datensätze entweder auf CNAME- oder TXT-Datensätze beziehen, je nachdem, welche Form von DKIM Sie verwendet haben. Easy DKIM verwendet CNAME-Datensätze und Bring Your Own DKIM (BYODKIM) verwendet TXT-Datensätze. Es werden detaillierte Verifizierungsverfahren für Easy DKIM und BYODKIM bereitgestellt.

Häufige Probleme mit der Domänenverifizierung

Wenn Sie versuchen, eine Domäne mit dem in the section called “Verifizieren einer Domänenidentität” beschriebenen Verfahren zu verifizieren, und Probleme auftreten, prüfen Sie die möglichen Ursachen und folgenden Lösungen.

- Sie versuchen, eine Domäne zu verifizieren, die Ihnen nicht gehört – Sie können Domänen, die Ihnen nicht gehören, nicht verifizieren. Wenn Sie beispielsweise eine E-Mail über Amazon SES von einer Adresse in der Domäne gmail.com senden möchten, müssen Sie diese E-Mail-Adresse gezielt verifizieren. Sie können nicht die gesamte Domäne gmail.com verifizieren.
- Sie versuchen, eine private Domäne zu verifizieren – Sie können eine Domäne nicht verifizieren, wenn die DNS-Datensätze nicht über öffentliches DNS aufgelöst werden können.

- Ihr DNS-Anbieter lässt Unterstriche in DNS-Datensatznamen nicht zu – Eine kleine Anzahl an DNS-Anbietern lässt nicht zu, dass Sie Unterstriche (_) in Datensatznamen einschließen. Der Unterstrich im DKIM-Datensatznamen ist jedoch erforderlich. Wenn Ihr DNS-Anbieter keine Unterstriche im Datensatznamen zulässt, bitten Sie das Kundensupport-Team des Anbieters um Hilfe.
- Ihr DNS-Anbieter hat den Domänennamen an das Ende des DNS-Datensatzes angehängt – Einige DNS-Anbieter hängen den Namen Ihrer Domäne automatisch an den Attributnamen des DNS-Datensatzes an. Wenn Sie z. B. einen Datensatz mit dem Attributnamen _domainkey.example.com erstellen, hängt der Anbieter möglicherweise den Domänennamen an, woraus sich _domainkey.example.com.example.com ergibt. Fügen Sie bei Eingabe des DNS-Datensatzes einen Punkt an das Ende des Domänennamens an, um doppelte Domänennamen zu vermeiden. Damit geben Sie Ihrem DNS-Anbieter zu verstehen, dass es nicht erforderlich ist, den Domänennamen an den Datensatz anzuhängen.
- Ihr DNS-Anbieter hat den DNS-Datensatzwert geändert.Einige Anbieter ändern automatisch DNS-Datensatzwerte, um nur Kleinbuchstaben zu verwenden. Amazon SES verifiziert Ihre Domäne nur, wenn es einen Verifizierungsdatensatz erkennt, für den der Attributwert genau mit dem Wert übereinstimmt, den Amazon SES beim Start der Domäneneigentumsüberprüfung angegeben hat. Wenn der DNS-Anbieter für Ihre Domäne Ihre DNS-Datensatzwerte in ausschließlich Kleinbuchstaben ändert, wenden Sie sich an den DNS-Anbieter, um zusätzliche Unterstützung zu erhalten.
- Du möchtest dieselbe Domain mehrfach verifizieren — Möglicherweise musst du deine Domain mehrmals verifizieren, weil du in verschiedenen Regionen sendest oder weil du dieselbe Domain für den Versand von mehreren AWS Konten verwendest. Wenn Ihr DNS-Anbieter nicht mehr als einen DNS-Datensatz mit dem gleichen Attributnamen zulässt, können Sie möglicherweise dennoch zwei Domänen verifizieren. Wenn Ihr DNS-Anbieter dies zulässt, können Sie demselben DNS-Datensatz mehrere Attributwerte zuweisen. Beispiel: Wenn Ihr DNS von Amazon Route 53 verwaltet wird, können Sie mit dem folgenden Verfahren mehrere Werte für denselben CNAME-Datensatz einrichten:

  1. Wählen Sie in der Route-53-Konsole den CNAME-Datensatz aus, den Sie bei der Verifizierung Ihrer Domäne in der ersten Region erstellt haben.
  2. Navigieren Sie im Feld Value (Wert) zum Ende des vorhandenen Attributwertes und drücken Sie dann die Eingabetaste.
  3. Fügen Sie den Attributwert für die zusätzliche Region hinzu und speichern Sie dann den Datensatz.

Wenn Ihr DNS-Anbieter nicht gestattet, demselben DNS-Datensatz mehrere Werte zuzuweisen, können Sie die Domäne einmal mit _domainkey im Attributnamen des DNS-Datensatzes und ein weiteres Mal ohne _domainkey im Attributnamen verifizieren. Der Nachteil dieser Lösung besteht darin, dass Sie dieselbe Domäne nur zweimal verifizieren können.

Überprüfen der Einstellungen für die Domänenverifizierung

Anhand des folgenden Verfahrens können Sie überprüfen, ob Ihr DNS-Datensatz zur Amazon-SES-Domänenverifizierung ordnungsgemäß auf Ihrem DNS-Server veröffentlicht wurde. Dieses Verfahren verwendet das Tool nslookup, das für Windows und Linux verfügbar ist. Unter Linux können Sie auch dig verwenden.

Die Befehle in dieser Anweisung wurden unter Windows 7 ausgeführt und die eingesetzte Beispieldomäne ist ses-example.com, die mit Easy DKIM konfiguriert wurde, was CNAME-Datensätze verwendet.

In diesem Verfahren müssen Sie zunächst die für Ihre Domäne zuständigen DNS-Server suchen und anschließend diese Server abfragen, um die CNAME-Datensätze anzuzeigen. Sie fragen die DNS-Server ab, die Ihre Domain bedienen, weil diese Server die meisten up-to-date Informationen für Ihre Domain enthalten. Es kann einige Zeit dauern, bis sie auf andere DNS-Server übertragen werden.

So überprüfen Sie, ob Ihre CNAME-Datensätze für die Domänenverifizierung auf Ihrem DNS-Server veröffentlicht werden

1. Führen Sie die folgenden Schritte aus, um die Nameserver für Ihre Domäne zu finden.

   a. Wechseln Sie zur Befehlszeile. Navigieren Sie unter Windows 7 zur Befehlszeile, indem Sie Start auswählen und anschließend cmd eingeben. Öffnen Sie auf Linux-basierten Betriebssystemen ein Terminalfenster.

   b. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein. Dabei ist <domain> Ihre Domäne. Dadurch werden alle Nameserver für Ihre Domäne aufgelistet.

   ```
   nslookup -type=NS <domain>
   ```

   Wenn Ihre Domäne ses-example.com lautet, sieht dieser Befehl wie folgt aus:

   ```
   nslookup -type=NS ses-example.com
   ```

In der Ausgabe des Befehls werden alle Nameserver für Ihre Domäne aufgelistet. Im nächsten Schritt werden Sie einen dieser Server abfragen.

2. Verifizieren Sie anhand der folgenden Schritte, ob die CNAME-Datensätze korrekt veröffentlicht wurden. Denken Sie daran, dass Amazon SES drei CNAME-Datensätze für die Easy-DKIM-Authentifizierung generiert. Wiederholen Sie daher die folgenden Verfahren für jeden der drei Datensätze.

   a. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein. Dabei ist **<random string>** der von SES generierte CNAME-Name, **<domain>** Ihre Domäne und **<name server>** einer der Nameserver, die Sie in Schritt 1 ermittelt haben.

   ```
   nslookup -type=CNAME <random string>._domainkey.<domain> <name server>
   ```

   Wenn in unserem ses-example.com-Beispiel in Schritt 1 ein Nameserver mit dem Namen ns1.name-server.net gefunden wurde und der von SES generierte **<random string>** `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz` lautet, geben Sie also Folgendes ein:

   ```
   nslookup -type=CNAME 4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com
    ns1.name-server.net
   ```

   b. Überprüfen Sie in der Ausgabe des Befehls, ob die Zeichenfolge nach `canonical name =` mit dem CNAME-Wert übereinstimmt, der bei Auswahl der Domäne in der Liste „Identities“ (Identitäten) in der Amazon-SES-Konsole angezeigt wird.

   In diesem Beispiel suchen wir unter `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz`_domainkey.ses-example.com einen CNAME-Datensatz mit dem Wert `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz.dkim.amazonses.com`. Wenn der Datensatz ordnungsgemäß veröffentlicht wurde, wird folgende Befehlsausgabe erwartet:

   ```
   4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com canonical name =
    "4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz.dkim.amazonses.com"
   ```

Häufige Probleme bei der E-Mail-Verifizierung

- Die Verifizierungs-E-Mail ist nicht eingegangen - Wenn Sie das in Verifizieren der Identität einer E-Mail-Adresse beschriebene Verfahren durchführen, innerhalb weniger Minuten jedoch keine Verifizierungs-E-Mail erhalten, führen Sie die folgenden Schritte aus:
  - Überprüfen Sie den Spam- oder Junk-Ordner für die E-Mail-Adresse, die Sie verifizieren möchten.
  - Vergewissern Sie sich, dass die Adresse, die Sie zu verifizieren versuchen, E-Mails empfangen kann. Senden Sie mittels einer separaten E-Mail-Adresse (z. B. Ihrer persönlichen E-Mail-Adresse) eine Test-E-Mail an die Adresse, die Sie verifizieren möchten.
  - Überprüfen Sie die Liste verifizierter Adressen in der Amazon SES-Konsole. Stellen Sie sicher, dass die E-Mail-Adresse, die Sie verifizieren möchten, fehlerfrei ist.

Beheben von DKIM-Problemen in Amazon SES

In diesem Abschnitt werden einige der Probleme aufgeführt, die während der Konfiguration der DKIM-Authentifizierung in Amazon SES auftreten können. Wenn während der Einrichtung von DKIM Probleme auftreten, prüfen Sie die möglichen Ursachen und Lösungen unten.

Sie haben DKIM erfolgreich eingerichtet, Ihre Nachrichten sind jedoch nicht mit einer DKIM-Signatur versehen.

Wenn Sie Easy DKIM oder BYODKIM zum Konfigurieren von DKIM für eine Domäne verwendet haben, die von Ihnen gesendeten Nachrichten jedoch nicht mit einer DKIM-Signatur versehen sind, führen Sie die folgenden Schritte aus:

- Stellen Sie sicher, dass DKIM für die entsprechende Identität aktiviert ist. Aktivieren Sie DKIM für eine Identität in der Amazon SES-Konsole, indem Sie die E-Mail-Domäne in der Liste Identities (Identitäten) auswählen. Erweitern Sie auf der Seite "Details" der Domäne den Eintrag DKIM und wählen Sie anschließend Enable (Aktivieren), um DKIM zu aktivieren.
- Stellen Sie sicher, dass Sie nicht von einer verifizierten E-Mail-Adresse in derselben Domäne aus senden. Wenn Sie DKIM für eine Domäne einrichten, sind alle Nachrichten, die Sie von dieser Domäne aus senden, mit einer DKIM-Signatur versehen, außer E-Mail-Adressen, die Sie gesondert verifiziert haben. Individuell verifizierte E-Mail-Adressen verwenden separate Einstellungen. Wenn Sie beispielsweise DKIM für die Domäne example.com konfiguriert und die E-Mail-Adresse mary@example.com gesondert verifiziert (DKIM für die Adresse jedoch nicht konfiguriert) haben, werden E-Mail-Nachrichten, die Sie von mary@example.com aus senden,

ohne DKIM-Authentifizierung gesendet. Sie können dieses Problem beheben, indem Sie die E-Mail-Adresse aus der Liste der Identitäten für Ihr Konto löschen.

- Wenn Sie dieselbe Identität in mehr als einer AWS Region verwenden, müssen Sie DKIM für jede Region separat konfigurieren. Ebenso müssen Sie DKIM für jedes AWS Konto konfigurieren, wenn Sie dieselbe Domain mit mehr als einem Konto verwenden. Wenn Sie die erforderlichen DNS-Einträge für eine spezifische Region oder ein spezifisches Konto entfernen, deaktiviert Amazon SES die DKIM-Signierung für diese Region oder dieses Konto. Wenn die DKIM-Signierung deaktiviert wird, sendet Amazon SES Ihnen eine Benachrichtigung per E-Mail.

Die DKIM-Details Ihrer Domäne werden in der Amazon SES-Konsole wie folgt angezeigt: DKIM: waiting on sender verification... DKIM-Verifizierungsstatus: Verifizierung ausstehend.

Wenn Sie die Verfahren in Easy DKIM oder BYODKIM - Verwendung Ihrer eigenen DKIM zur Konfiguration von DKIM für eine Domäne abschließen, die Amazon SES-Konsole jedoch weiterhin eine ausstehende DKIM-Verifizierung anzeigt, führen Sie die folgenden Schritte aus:

- Warten Sie bis zu 72 Stunden. In seltenen Fällen kann es einige Zeit dauern, bis die DNS-Datensätze in Amazon SES angezeigt werden.
- Bestätigen Sie, dass der CNAME-Datensatz (für Easy DKIM) oder der TXT-Datensatz (für BYODKIM) den richtigen Namen verwendet. Einige DNS-Anbieter hängen den Domänennamen automatisch an die von Ihnen erstellten Datensätze an. Wenn Sie beispielsweise einen Datensatz mit dem Namen `example._domainkey.example.com` erstellen, fügt Ihr DNS-Anbieter möglicherweise den Namen Ihrer Domäne am Ende dieser Zeichenfolge hinzu. Das Ergebnis sieht folgendermaßen aus: `example._domainkey.example.com.example.com`. Weitere Informationen finden Sie in der Dokumentation zu Ihrem DNS-Anbieter.

Sie erhalten eine E-Mail von Amazon SES mit der Mitteilung, dass Ihre DKIM-Einrichtung widerrufen wurde (oder wird).

Dies bedeutet, dass Amazon SES die erforderlichen CNAME-Datensätze (wenn Sie Easy DKIM verwendet haben) oder die erforderlichen TXT-Datensätze (wenn Sie BYODKIM verwendet haben) nicht mehr auf Ihrem DNS-Server finden kann. In der Benachrichtigungs-E-Mail wird Ihnen der Zeitraum mitgeteilt, in dem Sie die DNS-Datensätze erneut veröffentlichen müssen, bevor Ihr DKIM-Einrichtungsstatus widerrufen und die DKIM-Signierung deaktiviert wird. Wenn die DKIM-Einrichtung widerrufen wird, müssen Sie den DKIM-Einrichtungsprozess vollständig neu durchführen.

Beim Versuch, BYODKIM einzurichten, schlägt der DKIM-Verifizierungsprozess fehl.

Stellen Sie sicher, dass Ihr privater Schlüssel das richtige Format aufweist. Der private Schlüssel muss das Format PKCS #1 oder PKCS #8 aufweisen und 1024- oder 2048-Bit-RSA-Verschlüsselung verwenden. Darüber hinaus muss der private Schlüssel base64-codiert sein.

Beim Einrichten von BYODKIM erhalten Sie die Fehlermeldung **`BadRequestException`**, wenn Sie versuchen, einen öffentlichen Schlüssel für die Domäne anzugeben.

Wenn die Fehlermeldung `BadRequestException` angezeigt wird, gehen Sie folgendermaßen vor:

- Stellen Sie sicher, dass der Selektor, den Sie für den öffentlichen Schlüssel angeben, mindestens ein und maximal 63 alphanumerische Zeichen enthält. Der Selektor kann keine Punkte oder andere Symbole oder Satzzeichen enthalten.
- Stellen Sie sicher, dass Sie die Kopf- und Fußzeilen sowie alle Zeilenumbrüche aus dem öffentlichen Schlüssel entfernt haben.

Wenn Sie Easy DKIM verwenden, geben Ihre DNS-Server erfolgreich die Einträge zu DKIM CNAME in Amazon SES zurück, für den TXT-Datensatz zur Domain-Verifizierung geben sie jedoch **`SERVFAIL`** zurück.

Ihr DNS-Anbieter kann CNAME-Datensätze möglicherweise nicht umleiten. Amazon SES und ISPs Abfrage von TXT-Datensätzen. Um die DKIM-Spezifikation einzuhalten, müssen Ihre DNS-Server TXT-Datensatzabfragen sowie CNAME-Datensatzabfragen beantworten können. Wenn Ihr DNS-Anbieter nicht in der Lage ist, auf TXT-Datensatzabfragen zu antworten, können Sie Route 53 als DNS-Hosting-Anbieter verwenden.

Ihre E-Mails enthalten zwei DKIM-Signaturen

Die zusätzliche DKIM-Signatur, die `d=amazonses.com` enthält, wird automatisch von Amazon SES hinzugefügt. Sie können sie ignorieren.

> **Note**
>
> Microsoft Enterprise Outlook wählt nach dem Zufallsprinzip eine DKIM-Signatur für die Validierung aus, während die andere ignoriert wird. Dieses Verhalten scheint nicht mit der Reihenfolge zu korrelieren, in der die Signaturen angeordnet sind, sodass prozedurale Behelfslösungen unwirksam sind. SES kann nicht aufhören, E-Mails mit `amazonses.com` DKIM-Signaturen zu signieren, da diese für die Bearbeitung von Beschwerden erforderlich sind. Microsoft hat dies als bekanntes Problem anerkannt und es auf DNS-Auflösungsprobleme innerhalb seiner Infrastruktur zurückgeführt. Diese

Fehler bei der DNS-Auflösung würden erklären, warum die Überprüfung der DKIM-Signatur offenbar zufällig fehlschlägt, da öffentliche Schlüssel aus DNS-Einträgen abgerufen werden.

Amazon SES-Zustellungsprobleme

Nachdem Ihre Anforderung an Amazon SES erfolgreich war, wird Ihre Nachricht häufig sofort gesendet. In anderen Fällen kann es zu einer kurzen Verzögerung kommen. In jedem Fall können Sie sich darauf verlassen, dass Ihre E-Mail-Adresse gesendet wird.

Wenn Amazon SES Ihre Nachricht sendet, können jedoch mehrere Faktoren verhindern, dass sie erfolgreich zugestellt wird. In einigen Fällen bemerken Sie, dass die Zustellung fehlgeschlagen ist, nur wenn die Nachricht nicht angekommen ist. Gehen Sie folgendermaßen vor, um dieses Problem zu beheben.

Versuchen Sie Folgendes, wenn eine E-Mail nicht zugestellt wird:

- Überprüfen Sie, ob Sie eine `SendEmail`- oder `SendRawEmail`-Anforderung für die betreffende E-Mail erstellt und eine erfolgreiche Antwort erhalten haben. Wenn Sie diese Anforderungen programmgesteuert erstellen, überprüfen Sie Ihre Software-Protokolle, um sicherzustellen, dass das Programm die Anforderung erstellt und eine erfolgreiche Antwort erhalten hat.
- Lesen Sie den Blog-Artikel Three places where your email could get delayed when sending through SES, da es sich bei dem Problem eher um eine Verzögerung als um eine Nichtzustellung handeln kann.
- Prüfen Sie die E-Mail-Adresse des Absenders (die "From"-Adresse) auf ihre Gültigkeit. Überprüfen Sie außerdem Return-Path-Adresse. Dies ist die Adresse, an die Unzustellbarkeitsnachrichten gesendet werden. Wenn Ihre E-Mail unzustellbar ist, finden Sie dort eine erläuternde Fehlermeldung.
- Überprüfen Sie das AWS Service Health Dashboard, um zu bestätigen, dass kein bekanntes Problem mit Amazon SES vorliegt.
- Wenden Sie sich an den E-Mail-Empfänger oder ISP des Empfängers. Überprüfen Sie, ob der Empfänger die korrekte E-Mail-Adresse verwendet, und erkundigen Sie sich, ob irgendwelche Zustellungsprobleme mit dem ISP des Empfängers bekannt sind. Ermitteln Sie außerdem, ob die E-Mail angekommen ist, aber als Spam gefiltert wurde.
- Wenn Sie sich für einen gebührenpflichtigen AWS Support -Plan registriert haben, können Sie einen neuen technischen Support-Fall eröffnen. Bitte geben Sie in Ihrer Korrespondenz mit uns alle

relevanten Empfängeradressen zusammen mit allen Anfragen IDs oder Nachrichten an, die IDs Sie aus den `SendEmail` `SendRawEmail` Antworten erhalten haben.

- Warten Sie, um zu sehen, ob das Problem tatsächlich eine Verzögerung und nicht eine dauerhafte Unzustellbarkeit ist. Um Spammer zu bekämpfen, lehnen einige ISPs vorübergehend eingehende Nachrichten von unbekannten sendenden Mailservern ab. Dieser Prozess namens Greylisting kann die Zustellung verzögern. Amazon SES sendet diese Nachrichten erneut. Wenn Greylisting das Problem ist, wird der ISP die E-Mail möglicherweise bei einem dieser Wiederholungsversuche akzeptieren.
- Selbst wenn Sie die Interessen Ihrer Kunden im Auge behalten, können Sie immer noch auf Situationen stoßen, die sich auf die Zustellbarkeit Ihrer Nachrichten auswirken. Diethe section called “Aufrechterhaltung einer positiven Reputation als Absender” helfen Ihnen, sicherzustellen, dass Ihre E-Mail-Kommunikation Ihr Zielpublikum erreicht.

Probleme mit E-Mails von Amazon SES

In diesem Abschnitt werden einige häufige Probleme behandelt, die möglicherweise auftreten, wenn Sie E-Mails erhalten, die von Amazon SES gesendet wurden.

Der E-Mail-Client zeigt „gesendet via amazonses.com“ als Quelle der E-Mail an

Einige E-Mail-Clients zeigen die Domäne „via“ an, wenn die Domäne des Absenders nicht mit der Domäne übereinstimmt, von der die E-Mail gesendet wurde (in diesem Fall amazonses.com). Weitere Informationen finden Sie unter Zusätzliche Informationen neben dem Namen des Absenders auf der Gmail-Support-Website. Alternativ können Sie DomainKeys Identified Mail (DKIM) einrichten. Bei der Authentifizierung Ihrer E-Mails mit DKIM wird die Domäne „via“ in der Regel nicht von den E-Mail-Clients angezeigt, da die DKIM-Signatur zeigt, dass die E-Mail von der Domäne mit der angegebenen Identität stammt. Weitere Informationen zur Einrichtung von DKIM finden Sie unter Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES.

> **Note**
>
> Wenn Sie Spam oder andere unerwünschte E-Mail-Nachrichten von einem SES-Benutzer erhalten haben, verwenden Sie die Spam-Meldetools in Ihrem E-Mail-Client und führen Sie die Schritte zur Meldung von SES-E-Mail-Missbrauch aus, die unter Kontaktieren Sie uns aufgeführt sind.

Die Nachricht enthält unsinnige Zeichen bzw. Zeichenfolgen

Wenn Ihre Nachricht Zeichen enthält, die nicht im ASCII-Zeichensatz enthalten sind (z. B. lateinische Zeichen mit Akzenten, chinesische Zeichen oder arabische Zeichen), müssen Sie diese Zeichen mithilfe der HTML-Zeichenkodierung kodieren. Sie können webbasierte Tools verwenden, um die Zeichen in Ihrer E-Mail zu codieren, z. B. den HTML-Zeichenkonverter auf der Website „Email On Acid“.

Alternativ können Sie die MIME-Nachricht selbst zusammenstellen. In der MIME-Nachricht können Sie angeben, dass die Nachricht UTF-8-Codierung verwenden soll. Wenn Sie UTF-8-Codierung verwenden, können Sie Nicht-ASCII-Zeichen direkt in Ihren Nachrichten verwenden. Wenn Sie mit der Erstellung der MIME-Nachricht fertig sind, können Sie sie mithilfe der SendRawEmailAPI oder der SendMailAPI v2 senden.

Eine häufige Ursache für dieses Problem ist die Autoformatierungsfunktion zur Ersetzung von geraden durch typographische Anführungszeichen in Microsoft Word. Wenn Sie häufig Inhalte aus Word kopieren und in Ihre E-Mails einfügen, kann dieses Problem auftreten. Diese Funktion für intelligente Anführungszeichen ersetzt gerade Anführungszeichen ("... ") mit geschweiften Anführungszeichen („...“). Die geschweiften Anführungszeichen sind keine ASCII-Standardzeichen. Infolgedessen könnten sie in einigen E-Mail-Clients als "??" gerendert werden, oder als Gruppe von Zeichen, wie "â€œ". Um dieses Problem zu beheben, können Sie die Funktion für intelligente Anführungszeichen in Word deaktivieren. Alternativ können Sie die SendRawEmail Lösung aus dem vorherigen Absatz verwenden. Informationen zur Deaktivierung dieser Funktion finden Sie unter Intelligente Anführungszeichen in Word auf der Microsoft Office-Support-Website.

Probleme mit Amazon SES-Benachrichtigungen

Wenn Sie Probleme mit Unzustellbarkeits-, Beschwerde- oder Zustellbenachrichtigungen feststellen, prüfen Sie die unten aufgeführten möglichen Ursachen und Lösungen.

- Sie erhalten Unzustellbarkeitsbenachrichtigungen über Amazon SNS, wissen aber nicht, auf welche Empfänger sich diese Benachrichtigungen beziehen – In Zukunft haben Sie die folgenden Möglichkeiten, um eine Unzustellbarkeitsbenachrichtigung einem bestimmten Empfänger zuzuordnen:
  - Da Amazon SES keine von Ihnen hinzugefügten benutzerdefinierten Nachrichten IDs speichert, speichern Sie eine Zuordnung zwischen einer Kennung und der Amazon SES-Nachrichten-ID, die Amazon SES an Sie zurückgibt, wenn es die E-Mail akzeptiert.

  - Senden Sie in jedem Aufruf an Amazon SES an eine einzelne Person, anstatt eine einzelne Nachricht an mehrere Empfänger zu senden.
  - Sie können die Weiterleitung von Feedback per E-Mail aktivieren. Dadurch wird die vollständige Unzustellbarkeitsnachricht an Sie weitergeleitet.
- Sie erhalten Beschwerde- oder Lieferbenachrichtigungen über Amazon SNS oder die Weiterleitung von Feedback per E-Mail, wissen aber nicht, welchen Empfängern die Benachrichtigungen entsprechen. Manche ISPs redigieren die E-Mail-Adresse des beschwerten Empfängers, bevor sie die Beschwerdebenachrichtigung an Amazon SES weiterleiten. Damit Sie die E-Mail-Adresse des Empfängers finden können, empfiehlt sich eine Speicherung Ihres eigenen Mappings zwischen einer Kennung und der Amazon SES-Mitteilungs-ID, die Amazon SES beim Akzeptieren der E-Mail an Sie zurücksendet. Beachten Sie, dass Amazon SES keine von Ihnen hinzugefügten benutzerdefinierten Nachrichten IDs speichert.
- Sie möchten Benachrichtigungen einrichten, um zu einem Amazon SNS-Thema zu wechseln, dessen Eigentümer Sie nicht sind – Der Besitzer des Themas muss eine Amazon SNS-Zugriffsrichtlinie konfigurieren, die Ihr Konto berechtigt, die `SNS:Publish`-Aktion in seinem Thema aufzurufen. Weitere Informationen darüber, wie Sie den Zugriff auf Ihr Amazon SNS-Thema mithilfe von IAM-Richtlinien kontrollieren, finden Sie unter Verwaltung von Zugriffsberechtigungen für Ihre Amazon SNS-Themen im Amazon Simple Notification Service-Entwicklerleitfaden.

Fehler beim Senden von E-Mails über Amazon SES

In diesem Thema werden die Arten von versandspezifischen Fehlern besprochen, die beim Senden von E-Mails über Amazon SES auftreten können. Wenn Sie versuchen, eine E-Mail über Amazon SES zu senden, und der Aufruf an Amazon SES fehlschlägt, gibt Amazon SES eine Fehlermeldung an Ihre Anwendung zurück und die E-Mail wird nicht gesendet. Die Art und Weise, wie Sie diese Fehlermeldung erhalten, ist abhängig von der Art und Weise, wie Sie Amazon SES aufrufen.

- Wenn Sie die Amazon-SES-API direkt aufrufen, gibt die Abfrageaktion einen Fehler zurück. Der Fehler kann `MessageRejected` oder einer der Fehler sein, die im Thema Häufige Fehler der Amazon-Simple-Email-Service-API-Referenz angegeben sind.
- Wenn Sie Amazon SES mit einem AWS SDK aufrufen, das eine Programmiersprache verwendet, die Ausnahmen unterstützt, kann Amazon SES eine Ausnahme auslösen. Der Typ der Ausnahme ist abhängig von der SDK und dem Fehler. Die Ausnahme könnte beispielsweise ein Amazon SES `MessageRejectedException` (der tatsächliche Name kann je nach SDK variieren) oder eine

allgemeine AWS Ausnahme sein. Unabhängig vom Typ der Ausnahme erhalten Sie durch den Fehlertyp und die Fehlermeldung in der Ausnahme weitere Informationen.

- Wenn Sie Amazon SES über die SMTP-Schnittstelle aufrufen, hängt die Art und Weise, wie Sie die Fehler erhalten, von der Anwendung ab. Einige Anwendungen zeigen möglicherweise eine bestimmte Fehlermeldung an, andere nicht. Eine Liste der von Amazon SES zurückgegebenen SMTP-Antwortcodes finden Sie unter Von Amazon SES zurückgegebene SMTP-Antwortcodes.

> **Note**
>
> Wenn Ihr Aufruf zum Senden einer E-Mail an Amazon SES fehlschlägt, wird Ihnen diese E-Mail nicht in Rechnung gestellt.

Die folgenden Amazon-SES-spezifischen Problemtypen können dazu führen, dass Amazon SES eine Fehlermeldung zurückgibt, wenn Sie versuchen, eine E-Mail zu senden. Diese Fehler treten zusätzlich zu allgemeinen AWS Fehlern auf, `MalformedQueryString` wie sie im Thema Häufige Fehler der Amazon Simple Email Service API-Referenz beschrieben sind.

- Die E-Mail-Adresse wurde nicht verifiziert. Die folgenden Identitäten haben die Überprüfung in der Region region nicht bestanden: identity1, identity2, identity3 – Sie versuchen, eine E-Mail von einer E-Mail-Adresse oder Domäne zu senden, die Sie nicht mit Amazon SES verifiziert haben. Dieser Fehler kann für folgende Adressen gelten: "From", "Source", "Sender" oder "Return-Path". Wenn sich Ihr Konto noch in der Amazon-SES-Sandbox befindet, müssen Sie alle E-Mail-Adressen aller Empfänger verifizieren. Dies gilt nicht für Empfänger, die vom Amazon-SES-Postfachsimulator bereitgestellt werden. Wenn Amazon SES nicht alle fehlgeschlagenen Identitäten auflisten kann, endet die Fehlermeldung mit Auslassungspunkten.

  > **Note**
  >
  > Amazon SES hat mehrere Endpunkte AWS-Regionen, und der Bestätigungsstatus der E-Mail-Adresse ist für jeden AWS-Region separat. Sie müssen den Bestätigungsprozess für jeden Absender in dem, den AWS-Regionen Sie verwenden möchten, abschließen.

- Konto ist pausiert – Die Fähigkeit Ihres Kontos, E-Mails zu senden, ist pausiert. Sie können weiterhin auf die Amazon-SES-Konsole zugreifen und die meisten Operationen ausführen. Wenn Sie jedoch versuchen, eine E-Mail zu senden, erhalten Sie diese Nachricht.

Wenn wir die Fähigkeit eines Kontos zum Versenden von E-Mails unterbrechen, senden wir automatisch eine Benachrichtigung an die E-Mail-Adresse, die mit Ihrem AWS-Konto-Konto verknüpft ist. Weitere Informationen finden Sie unter the section called “Überprüfungsprozess für den Versand FAQs”.

- Drosselung – Ihre Anwendung versucht möglicherweise, zu viele Nachrichten pro Sekunde zu senden oder Sie haben während der letzten 24 Stunden möglicherweise zu viele E-Mails gesendet. In diesen Fällen kann die Fehlermeldung den folgenden Beispielen ähneln:
  - Tägliches Nachrichtenkontingent überschritten – Sie haben die für einen 24-Stunden-Zeitraum erlaubte maximale Anzahl von Nachrichten gesendet. Wenn Sie Ihr tägliches Kontingent überschritten haben, müssen Sie bis zum nächsten 24-Stunden-Zeitraum warten, bevor Sie weitere E-Mails senden können.
  - Maximale Senderate überschritten – Sie versuchen, mehr E-Mails pro Sekunde zu senden als von Ihrer maximalen Senderate zugelassen. Wenn Sie Ihre Senderate überschritten haben, können Sie weiterhin E-Mails senden, müssen jedoch die Senderate reduzieren. Weitere Informationen finden Sie im AWS Messaging and Targeting-Blog unter So gehen Sie mit dem Fehler „Drosselung — Maximale Senderate überschritten“ um.
  - Die maximale Sigv2-SMTP-Senderate wurde überschritten — Sie versuchen, Nachrichten mit SMTP-Anmeldeinformationen zu senden, die vor dem 10. Januar 2019 erstellt wurden. Ihre SMTP-Anmeldeinformationen wurden mit einer älteren Version der Signatur erstellt. AWS Aus Sicherheitsgründen sollten Sie Anmeldeinformationen, die Sie vor diesem Datum erstellt haben, löschen und durch neue Anmeldeinformationen ersetzen. Sie können ältere Anmeldeinformationen mit der IAM-Konsole löschen. Weitere Informationen zum Erstellen von Anmeldeinformationen finden Sie unter the section called “Abrufen Ihrer SMTP-Anmeldeinformationen”.

Sie sollten Ihre Sendeaktivitäten regelmäßig überwachen, um Ihre Sendekontingente im Auge zu behalten. Weitere Informationen finden Sie unter Überwachung Ihrer Amazon-SES-Sendekontingente. Allgemeine Informationen zu Sendekontingenten finden Sie unter Verwalten Ihrer Amazon SES Versandkontingente. Weitere Informationen zum Erhöhen Ihrer Sendekontingente finden Sie unter Erhöhen Ihrer Amazon-SES-Sendekontingente.

> **Important**
>
> Wenn der Fehlertext, in dem der Ablehnungsfehler erläutert wird, keinen Bezug zur Überschreitung des täglichen Kontingents oder der maximalen Senderate hat, könnte ein

systemweites Problem für die Begrenzung des Sendefunktionsumfangs vorliegen. Weitere Informationen zum Service-Status finden Sie auf dem AWS Service Health Dashboard.

- There are no recipients specified – Es wurden keine Empfänger angegeben.
- There are non-ASCII characters in the email address – Die E-Mail-Adresse muss eine 7-Bit-ASCII-Zeichenfolge sein. Wenn Sie E-Mails an oder von Adressen mit Unicode-Zeichen im Domänenteil der Adresse senden möchten, müssen Sie die Domäne über Punycode codieren. Punycode ist weder im lokalen Teil der E-Mail-Adresse (das ist der Teil vor dem @-Zeichen) noch im "friendly from"-Namen zulässig. Wenn Sie Unicode-Zeichen im „friendly from“-Namen verwenden möchten, müssen Sie diesen mit in MIME-kodierter Wort-Syntax wie in Senden von Roh-E-Mails mit der Amazon SES API v2 beschrieben kodieren. Weitere Informationen zu Punycode finden Sie unter RFC 3492.
- Mail FROM-Domäne ist nicht verifiziert – Amazon SES konnte den MX-Datensatz nicht lesen, der erforderlich ist, um die angegebene MAIL FROM-Domäne zu verwenden. Weitere Informationen zum Einrichten benutzerdefinierter MAIL FROM-Domänen finden Sie unter Verwenden einer benutzerdefinierten MAIL FROM-Domäne.
- Konfigurationssatz ist nicht vorhanden – Der von Ihnen angegebene Konfigurationssatz ist nicht vorhanden. Ein Konfigurationssatz ist ein optionaler Parameter, den Sie zum Veröffentlichen von E-Mail-Sendeereignissen verwenden. Weitere Informationen finden Sie unter Überwachen des E-Mail-Versands mithilfe der Amazon SES-Ereignisveröffentlichung.

Erhöhen des Durchsatzes mit Amazon SES

Wenn Sie Nachrichten senden, können Sie Amazon SES so oft aufrufen, wie es Ihre maximale Senderate erlaubt. (Weitere Informationen über Ihre maximale Senderate finden Sie unter Verwalten Ihrer Amazon SES Versandkontingente.) Allerdings benötigt jeder Aufruf an Amazon SES Zeit für die Ausführung.

Wenn Sie mehrere Amazon SES-Aufrufe mithilfe der Amazon SES-API oder der SMTP-Schnittstelle durchführen, können die folgenden Tipps Ihnen helfen, Ihren Durchsatz zu verbessern:

- Messen Sie Ihre aktuelle Leistung, um Engpässe zu erkennen – Bei einem möglichen Leistungstest senden Sie mehrere Test-E-Mails so schnell wie möglich innerhalb einer Codeschleife in Ihrer Anwendung. Messen Sie die Roundtrip-Latenzzeit für jede einzelne `SendEmail`-Anforderung. Starten Sie anschließend inkrementell weitere Instances der Anwendung auf demselben Computer und achten Sie auf eventuelle Auswirkungen auf die Netzwerklatenz. Sie können diesen Test auch

auf mehreren Computern und in verschiedenen Netzwerken ausführen, um mögliche Engpässe bei den Computerressourcen oder Netzwerkengpässe besser zu identifizieren.

- (Nur API) Verwenden Sie gegebenenfalls persistente HTTP-Verbindungen – Anstatt sich einen Mehraufwand durch das Herstellen separater neuer HTTP-Verbindungen für jede API-Anforderung einzuhandeln, verwenden Sie besser persistente HTTP-Verbindungen. Das bedeutet, dass dieselbe HTTP-Verbindung für mehrere API-Anforderungen wiederverwendet wird.
- Ziehen Sie die Verwendung mehrerer Threads in Betracht – Wenn eine Anwendung einen einzelnen Thread verwendet, ruft der Anwendungscode die Amazon SES-API auf und wartet dann gleichzeitig auf eine API-Antwort. Das Senden von E-Mails ist in der Regel eine I/O-intensive Operation. Mit dem Einsatz mehrerer Threads wird ein höherer Durchsatz erzielt. Sie können gleichzeitig senden und dabei beliebig viele Ausführungs-Threads verwenden.
- Ziehen Sie die Verwendung mehrerer Prozesse in Betracht – Die Verwendung mehrerer Prozesse kann helfen, den Durchsatz zu erhöhen, da Sie über mehr gleichzeitige aktive Verbindungen mit Amazon SES verfügen. Sie können z. B. Ihre geplanten E-Mails in mehrere Buckets segmentieren und dann mehrere Instances Ihres E-Mail-Sendeskripts gleichzeitig ausführen.
- Ziehen Sie die Verwendung eines lokalen E-Mail-Relays in Betracht – Ihre Anwendung kann Nachrichten an Ihren lokalen E-Mail-Server schnell übertragen. Dieser kann dann helfen, die Nachrichten zu puffern, und sie an Amazon SES asynchron übertragen. Einige E-Mail-Server unterstützen Zustellungsparallelität, was bedeutet, dass Ihr E-Mail-Server auch dann mehrere Threads beim Senden an Amazon SES verwendet, wenn Ihre Anwendung E-Mails an einen E-Mail-Server in einzelnen Threads generiert. Weitere Informationen finden Sie unter Integrieren von Amazon SES in Ihren vorhandenen E-Mail-Server.
- Erwägen Sie, Ihre Anwendung näher am Amazon SES SES-API-Endpunkt zu hosten — Möglicherweise möchten Sie erwägen, Ihre Anwendung in einem Rechenzentrum in der Nähe des Amazon SES SES-API-Endpunkts oder auf einer EC2 Amazon-Instance in derselben AWS Region wie der Amazon SES-API-Endpunkt zu hosten. Dies kann dazu beitragen, die Netzwerklatenz zwischen Ihrer Anwendung und Amazon SES zu verringern und den Durchsatz zu verbessern. Eine Liste der Regionen, in denen Amazon SES verfügbar ist, finden Sie unter Amazon Simple Email Service (Amazon SES) in der Allgemeine AWS-Referenz.
- Ziehen Sie die Verwendung mehrerer Computer in Betracht – Je nach Systemkonfiguration auf Ihrem Hostcomputer kann die Anzahl gleichzeitiger HTTP-Verbindungen mit einer einzelnen IP-Adresse begrenzt sein, was den Nutzen der Parallelität einschränkt, wenn Sie eine bestimmte Anzahl gleichzeitiger Verbindungen auf einem einzelnen Computer überschreiten. Wenn dies ein Engpass ist, denken Sie einmal über gleichzeitige Amazon SES-Anfragen mithilfe mehrerer Computer nach.

- Ziehen Sie die Verwendung der Amazon SES-Abfrage-API anstelle des SMTP-Endpunkts in Betracht – Wenn Sie die Amazon SES-Abfrage-API verwenden, können Sie die E-Mail-Sendeanforderung mit einem einzelnen Netzwerkaufruf absenden. Eine Verbindung mit dem SMTP-Endpunkt hingegen umfasst eine SMTP-Aushandlung, die aus mehreren Netzwerkanfragen besteht (z. B. EHLO, MAIL FROM, RCPT TO, DATA, QUIT). Weitere Informationen über die Amazon SES-Abfrage-API erhalten Sie unter Verwenden der Amazon-SES-API zum Senden von E-Mails.
- Verwenden Sie den Amazon SES-Postfachsimulator zum Testen des maximalen Durchsatzes – Sie können mithilfe des Postfachsimulators alle Änderungen testen, die Sie implementieren möchten. Der Postfachsimulator kann Ihnen beim Ermitteln des maximalen Durchsatzes Ihres Systems helfen, ohne dafür Ihre tägliche Sendequote zu verbrauchen. Informationen zum Postfachsimulator finden Sie unter Manuelles Verwenden des Postfachsimulators.

Für den Fall, dass Sie auf Amazon SES über die SMTP-Schnittstelle zugreifen, erhalten Sie unter SMTP-Probleme bei Amazon SES weitere Informationen zu spezifischen SMTP-bezogenen Problemen, die den Durchsatz beeinflussen können.

SMTP-Probleme bei Amazon SES

Dieser Abschnitt enthält Lösungen für mehrere häufig auftretende Probleme im Zusammenhang mit dem Senden von E-Mail-Nachrichten über die Amazon-SES-SMTP-Schnittstelle (Simple Mail Transfer Protocol). Er enthält auch eine Liste von SMTP-Antwortcodes, die von Amazon SES zurückgegeben werden.

Weitere Informationen zum Senden von E-Mail-Nachrichten über die Amazon-SES-SMTP-Schnittstelle finden Sie unter Verwenden der Amazon-SES-SMTP-Schnittstelle zum Senden von E-Mails.

- Sie können keine Verbindung zum Amazon-SES-SMTP-Endpunkt herstellen.

  Probleme beim Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt stehen meist mit folgenden Problemen im Zusammenhang:

  - Falsche Anmeldeinformationen — Die Anmeldeinformationen, die Sie für die Verbindung mit dem SMTP-Endpunkt verwenden, unterscheiden sich von Ihren AWS Anmeldeinformationen. Informationen zum Abrufen Ihrer SMTP-Anmeldeinformationen finden Sie unter Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen. Weitere Informationen zu Anmeldeinformationen finden Sie unter Arten von Amazon-SES-Anmeldeinformationen.

- Netzwerk- oder Firewall-Probleme – Möglicherweise blockiert Ihr Netzwerk ausgehende Verbindungen über den Port, über den Sie E-Mails senden möchten. Um festzustellen, ob ein Problem in Ihrem lokalen Netzwerk die Verbindungsprobleme verursacht, geben Sie in der Befehlszeile den folgenden Befehl ein, wobei Sie *port* durch den Port ersetzen, den Sie zu verwenden versuchen (normalerweise 465, 587, 2465 oder 2587): `telnet email-smtp.us-west-2.amazonaws.com port`

  Wenn Sie mit diesem Befehl eine Verbindung mit dem SMTP-Server herstellen können und Sie versuchen, mithilfe von TLS Wrapper oder STARTTLS eine Verbindung mit Amazon SES herzustellen, führen Sie die in Testen der Verbindung zur Amazon-SES-SMTP-Schnittstelle über die Befehlszeile gezeigten Verfahren durch.

  Wenn Sie keine Verbindung mit dem Amazon-SES-SMTP-Endpunkt über `telnet` oder `openssl` herstellen können, ist dies ein Hinweis darauf, dass etwas in Ihrem Netzwerk (wie etwa eine Firewall) ausgehende Verbindungen über den von Ihnen verwendeten Port blockiert. Versuchen Sie gemeinsam mit Ihrem Netzwerkadministrator, das Problem zu diagnostizieren und zu beheben.

- Sie senden von einer Amazon-EC2-Instance über Port 25 an Amazon SES, und Sie erhalten Timeout-Fehler.

  Amazon EC2 schränkt Port 25 standardmäßig ein. Um diese Beschränkungen aufzuheben, senden Sie eine Amazon EC2 Anforderung zum Entfernen von E-Mail-Sendebeschränkungen ab. Sie können auch eine Verbindung mit Amazon SES über Port 465 oder Port 587 herstellen. Beide sind nicht eingeschränkt.

- E-Mails gehen durch Netzwerkfehler verloren.

  Stellen Sie sicher, dass Ihre Anwendung eine Logik für Wiederholversuche verwendet, wenn sie eine Verbindung mit dem Amazon-SES-SMTP-Endpunkt herstellt. Außerdem muss die Anwendung die Übertragung von Nachrichten erkennen und im Fall eines Netzwerkfehlers wiederholen können. SMTP ist ein Verbose-Protokoll. Das Senden von E-Mails mit diesem Protokoll erfordert mehrere Netzläufe. Aufgrund der Beschaffenheit von SMTP nimmt die Möglichkeit von Netzwerkfehlern zu.

- Die Verbindung mit dem SMTP-Endpunkt geht verloren.

  Verlorene Verbindungen werden am häufigsten durch die folgenden Probleme verursacht:

  - MTU-Größe – Wenn Sie eine Timeout-Fehlermeldung erhalten, ist möglicherweise die maximale Größe für Übertragungseinheiten (Maximum Transmission Unit, MTU) der Netzwerkschnittstelle für den Computer, mit dem Sie eine Verbindung mit der Amazon-SES-SMTP-Schnittstelle

herstellen, zu hoch. Legen Sie, um dieses Problem zu lösen, die MTU-Größe auf diesem Computer auf 1500 Byte fest.

Weitere Informationen über das Festlegen der MTU-Größe auf Microsoft Windows-, Linux- und macOS-Betriebssystemen finden Sie unter Abfragen scheinen zu hängen und erreichen den Cluster nicht im Amazon Redshift Verwaltungsleitfaden.

Weitere Informationen zur Einstellung der MTU-Größe für eine Amazon EC2 EC2-Instance finden Sie unter Network Maximum Transmission Unit (MTU) für Ihre EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch.

- Langlebige Verbindungen – Der Amazon-SES-SMTP-Endpunkt wird auf einer Flotte von Amazon-EC2-Instances hinter einem Elastic Load Balancer (ELB) ausgeführt. Um sicherzustellen, dass das System fehlertolerant ist up-to-date, werden aktive Amazon EC2 EC2-Instances regelmäßig beendet und durch neue Instances ersetzt. Da Ihre Anwendung eine Verbindung mit einer Amazon-EC2-Instance über die ELB herstellt, ist die Verbindung nicht mehr gültig, wenn die Amazon-EC2-Instance beendet wird. Sie sollten eine neue SMTP-Verbindung einrichten, nachdem Sie eine feste Anzahl von Nachrichten über eine einzelne SMTP-Verbindung gesendet haben, oder wenn die SMTP-Verbindung für einen bestimmten Zeitraum aktiv war. Sie werden etwas experimentieren müssen, um geeignete Schwellenwerte basierend darauf zu ermitteln, wo Ihre Anwendung gehostet wird und wie diese E-Mails an Amazon SES sendet.

- Sie möchten die IP-Adressen der Amazon-SES-SMTP-E-Mail-Server wissen, damit Sie die IP-Adressen in eine Zulassungsliste für Ihr Netzwerk eintragen können.

  Die IP-Adressen für die Amazon-SES-SMTP-Endpunkte befinden sich hinter der Lastenverteilung. Infolgedessen ändern sich diese IP-Adressen häufig. Es ist nicht möglich, eine endgültige Liste aller IP-Adressen für die Amazon-SES-Endpunkte bereitzustellen. Wir empfehlen Ihnen, die Zulassungsliste der `amazonses.com`-Domain, anstatt der Auflistung einzelner zugelassener IP-Adressen.

Von Amazon SES zurückgegebene SMTP-Antwortcodes

Dieser Abschnitt enthält eine Liste der von der Amazon-SES-SMTP-Schnittstelle zurückgegebenen Antwortcodes.

SMTP-Anforderungen, die 400-Fehler erhalten, sollten Sie wiederholen. Wir empfehlen, dass Sie ein System implementieren, das Anforderungen mit progressiv verlängerten Wartezeiten wiederholt (z. B.

5 Sekunden warten bis zur Wiederholung, dann 10 Sekunden und dann 30 Sekunden warten). Wenn die dritte Wiederholung nicht erfolgreich war, 20 Minuten warten und anschließend den Vorgang wiederholen. Ein Beispiel für eine Implementierung, die eine exponentielle Wiederholungsrichtlinie verwendet, finden Sie im Artikel Umgang mit dem Fehler „Drosselung- Maximale Senderate überschritten“ im AWS zu Messaging und Targeting.

> **Note**
>
> AWS SDKs implementieren die Wiederholungslogik automatisch, sie verwenden jedoch die HTTPS-Schnittstelle anstelle von SMTP.

Wenn Sie einen 500-Fehler erhalten, müssen Sie Ihre Anforderung überarbeiten ein Problem beheben, bevor Sie die Anforderung erneut senden. Wenn Ihre AWS Authentifizierungsdaten beispielsweise ungültig sind, müssen Sie Ihre Anwendung so aktualisieren, dass sie die richtigen Anmeldeinformationen verwendet, bevor Sie Ihre Anfrage erneut einreichen.

Description	Antwortcode	Weitere Informationen
Authentifizierung erfolgreich	`235 Authentication successful`	Ihr SMTP-Client hat erfolgreich eine Verbindung mit dem SMTP-Server hergestellt und sich angemeldet.
Erfolgreiche Zustellung	`250 Ok` *`MessageID`*	*`MessageID`* ist eine eindeutige Zeichenfolge, die Amazon SES verwendet, um eine Nachricht zu identifizieren.
Service nicht verfügbar	`421 Too many concurrent SMTP connections`	Amazon SES kann die Anforderung nicht verarbeiten, weil zurzeit zu viele Verbindungen mit dem SMTP-Server hergestellt sind.
Lokaler Verarbeitungsfehler	`451 Temporary service failure`	Amazon SES konnte die Anforderung nicht verarbeiten. Mit der Anforderung gibt es

Description	Antwortcode	Weitere Informationen
		möglicherweise Probleme, die die Verarbeitung verhindern.
Zeitüberschreitung	`451 Timeout waiting for data from client`	Es ist zu viel Zeit zwischen den Anfragen verstrichen, sodass der SMTP-Server die Verbindung beendet hat.
Sendequote pro Tag überschritten	`454 Throttling failure: Daily message quota exceeded`	Die in Amazon SES zulässige maximale Anzahl von E-Mails, die Sie in einem Zeitraum von 24 Stunden senden können, wurde überschritten. Weitere Informationen finden Sie unter Verwalten Ihrer Amazon SES Versandkontingente.
Maximale Senderate überschritten	`454 Throttling failure: Maximum sending rate exceeded`	Die in Amazon SES zulässige maximale Anzahl von E-Mails, die Sie pro Sekunde senden können, wurde überschritten. Weitere Informationen finden Sie unter Verwalten Ihrer Amazon SES Versandkontingente.

Description	Antwortcode	Weitere Informationen
Amazon-SES-Problem bei der Validierung von SMTP-Anmeldeinformationen	`454 Temporary authentication failure`	Zu den Problemen, die dazu führen, dass dieses Problem auftritt, gehören unter anderem: • Es liegt ein Problem mit der Verschlüsselung zwischen Ihrer E-Mail-Anwendung und Amazon SES vor. Beachten Sie, dass Sie eine verschlüsselte Verbindung verwenden müssen, wenn Sie eine Verbindung mit Amazon SES herstellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit dem Amazon-SES-SMTP-Endpunkt. • In Amazon SES könnte ein Problem aufgetreten sein. Überprüfen Sie das AWS Service Health Dashboard auf Aktualisierungen.
Probleme mit dem Eingang der Anforderung	`454 Temporary service failure`	Amazon SES konnte die Anforderung nicht erfolgreich empfangen. Demzufolge wurde die Nachricht nicht gesendet.
Falsche Anmeldeinformationen	`530 Authentication required`	Die Anwendung, die Sie zum Senden von E-Mails verwenden, hat beim Verbindungsaufbau keine Authentifizierung bei der Amazon-SES-SMTP-Schnittstelle durchgeführt.

Description	Antwortcode	Weitere Informationen
Ungültige Anmeldeinformationen für die Authentifizierung	`535 Authentication Credentials Invalid`	Die Anwendung, die Sie zum Senden von E-Mails verwenden, hat für Amazon SES keine gültigen SMTP-Anmeldeinformationen bereitgestellt. Beachten Sie, dass Ihre SMTP-Anmeldeinformationen nicht mit Ihren AWS Anmeldeinformationen identisch sind. Weitere Informationen finden Sie unter Abrufen Ihrer Amazon-SES-SMTP-Anmeldeinformationen.
Konto hat Amazon SES nicht abonniert	`535 Account not subscribed to SES`	AWS-Konto Derjenige, der die SMTP-Anmeldeinformationen besitzt, ist nicht für Amazon SES angemeldet.
Nachricht ist zu lang	`552 Message is too long.`	Die Nachricht, die Sie senden möchten, ist größer als die Maximalgröße für Nachrichten.
Konto hat Amazon SES nicht abonniert	`535 Account not subscribed to SES`	AWS-Konto Derjenige, der die SMTP-Anmeldeinformationen besitzt, ist nicht für Amazon SES angemeldet.
„MAIL FROM“-Syntaxfehler	`553 <email-address> Invalid email address`	Es gibt einen Syntaxfehler im „MAIL FROM“-Teil der SMTP-Nachricht. Bitte vergewissern Sie sich, dass Sie das richtige Format befolgen und vergessen Sie nicht, die E-Mail-Adresse in „<>“ einzuschließen.

Description	Antwortcode	Weitere Informationen
„RCPT TO“-Syntaxfehler	`553 <email-address > address unknown`	Es gibt einen Syntaxfehler im „RCPT TO“-Teil der SMTP-Nachricht. Bitte vergewissern Sie sich, dass Sie das richtige Format befolgen und vergessen Sie nicht, die E-Mail-Adresse in „**<>**“ einschließen.
Benutzer zum Aufrufen des Amazon-SES-SMTP-Endpunkts nicht autorisiert	`554 Access denied: User UserARN is not authorized to perform ses:SendRawEmail on resource IdentityARN`	Die AWS Identity and Access Management (IAM-) Richtlinie oder die Amazon SES SES-Versandautorisierungsrichtlinie des Benutzers, der Eigentümer der SMTP-Anmeldeinformationen ist, darf den Amazon SES SES-SMTP-Endpunkt nicht aufrufen.

Description	Antwortcode	Weitere Informationen
Nicht verifizierte E-Mail-Adresse	`554 Message rejected: Email address is not verified. The following identities failed the check in region` *`region`*`: `*`identity0`*` , `*`identity1`*` , `*`identity2`*	Sie versuchen, eine E-Mail von einer E-Mail-Adresse oder Domäne zu senden, die nicht für das Senden von E-Mails von Ihrem Amazon-SES-Konto verifiziert wurde. Dieser Fehler kann für folgende Adressen gelten: „From“, „Source“, „Sender“ oder „Return-Path“. Wenn sich Ihr Konto noch in der Sandbox befindet, müssen Sie alle E-Mail-Adressen aller Empfänger verifizieren. (Dies gilt nicht für Empfänger, die vom Amazon-SES-Postfachsimulator bereitgestellt werden.) Sofern Amazon SES nicht alle bei der Verifizierungsüberprüfung fehlgeschlagenen Identitäten anzeigen kann, endet die Fehlermeldung mit drei Punkten (...). **Note** Amazon SES hat mehrere Endpunkte AWS-Regionen, und der Bestätigungsstatus der E-Mail-Adresse ist für jeden AWS-Region separat. Sie müssen den Bestätigungsprozess für jeden Absender in dem AWS-Regionen , den

Description	Antwortcode	Weitere Informationen
		Sie verwenden möchten, abschließen.

> **Note**
>
> Probieren Sie bei SMTP-Problemen, die durch die Fehlerbehebung auf dieser Seite nicht behoben wurden, die SES-Supportoptionen aus, die unter Kontaktieren Sie uns aufgeführt sind.

Häufig gestellte Fragen zu Amazon SES (FAQs)

In diesem Abschnitt finden Sie Antworten auf häufig gestellte Fragen zur Nutzung von Amazon SES.

Dieser Abschnitt enthält FAQs die folgenden Themen:

- Dedizierte IP-Adressen (verwaltet) FAQs
- Amazon SES Versandprüfungsprozess FAQs
- DNS-Blackhole-Liste (DNSBL) FAQs
- Amazon SES SES-Metriken zum Senden von E-Mails FAQs

Dedizierte IP-Adressen (verwaltet) FAQs

Es Dedizierte IP-Adressen (verwaltet) bietet zwar zahlreiche automatisierte Funktionen für dediziertes IP-Management, Skalierung und Warmup, aber es gab einige Missverständnisse über den Umfang dieser Automatisierung und die Aufgaben von SES. Es wäre falsch anzunehmen, dass „verwaltet“ bedeutet, dass SES sich vollständig um alle Aspekte der IP-Reputation und der Börsennotierung kümmert. Um diese Missverständnisse auszuräumen, müssen wir betonen, dass der Service zwar technische Aspekte wie Skalierung und Aufwärmphase automatisiert, Sie aber weiterhin dafür verantwortlich sind, Ihre Senderreputation aufrechtzuerhalten und alle Probleme im Zusammenhang mit der Reputation zu lösen, z. B. die Aufnahme in eine Reputation Block List (RBL).

Damit werden häufig FAQs vorkommende Missverständnisse über den Umfang der Funktion ausgeräumt und das Modell der gemeinsamen Verantwortung zwischen Ihnen und SES verdeutlicht. In diesen häufig gestellten Fragen wird darauf hingewiesen, dass sich der Aspekt „gemanagt“ zwar auf die Verwaltung der technischen Infrastruktur bezieht, Sie jedoch Ihren Ruf als Absender aktiv überwachen und pflegen, die Absprungraten niedrig halten und die meisten Anfragen zum Löschen von RBLs von der Liste selbst bearbeiten müssen.

F1. Kann ich SES bitten, meine dedizierte IP-Adresse (verwaltet) von der Liste in einer RBL zu streichen?

Wenn Ihre dedizierte IP-Adresse (verwaltet) in einer RBL von E-Mail-Empfängern aufgeführt ist, liegt dies nicht in der Verantwortung von SES. Sie müssen die Entfernung selbst beim RBL-Administrator beantragen. Es ist wichtig, dass Sie Ihre zugewiesenen IPs (verwalteten) Daten überwachen, indem Sie sowohl Bounce-Benachrichtigungen als auch SMTP-Antwortnachrichten verfolgen, um Blockaden

zu identifizieren. Diese Überwachung trägt dazu bei, Ihren Ruf als E-Mail-Versender zu schützen, und ermöglicht es Ihnen, etwaige RBL-Vorfälle schnell zu beheben und so eine konsistente E-Mail-Zustellbarkeit sicherzustellen.

F2. Kann ich SES bitten, eine neue dedizierte IP-Adresse (verwaltet) zuzuweisen, die eine aktuelle IP-Adresse ersetzt, die in einer RBL aufgeführt ist, die nicht von Spamhaus angeboten wird?

Nein. SES rotiert keine dedizierten IP-Adressen. Da Sie für Ihre dedizierten IP-Adressen, ob verwaltete oder Standard-IP-Adressen, verantwortlich sind, müssen Sie herausfinden, warum sie in der RBL aufgeführt werden, und sie selbst von der Liste streichen lassen.

F3. Kann SES die Absprungrate einer dedizierten IP-Adresse (verwaltet) überwachen, die meinem Konto zugewiesen ist, und die Adresse wechseln, wenn die Absprungrate hoch wird?

Nein. SES wechselt keine dedizierten IP-Adressen, wenn ein Konto eine hohe Absprungrate aufweist. Wenn Sie eine dedizierte IP-Adresse (verwaltet) leasen, hat nur Ihr Konto das ausschließliche Recht, E-Mails über diese dedizierte IP-Adresse zu versenden, sodass SES Ihr Konto nicht überwachen kann. Es liegt in Ihrer Verantwortung, Ihren Ruf als Absender und Ihre E-Mail-Komponenten zu verwalten, einschließlich der Bearbeitung von Beschwerden und der Aufrechterhaltung einer Absprungrate von unter 2%.

F4. Ich habe gerade eine dedizierte IP-Adresse (verwaltet) geleast und die über sie gesendete E-Mail wird zurückgeschickt, weil die Adresse auf einer RBL steht. Prüft SES die Reputation einer dedizierten IP-Adresse (verwaltet), bevor es sie an ein Konto vermietet?

Ja. SES setzt jede dedizierte (verwaltete) IP-Adresse zurück (30 Tage), bevor sie an ein SES-Konto vermietet wird. Der Ruf wird in der Regel auf die meisten großen Anbieter zurückgesetzt. SES stellt sicher, dass die Adresse nicht in einer RBL steht, wie Spamhaus. SES überwacht jedoch nicht alle RBLs verfügbaren Adressen, z. B. kleinere, regionale Adressen. RBLs Falls Sie aufgrund einer B2B-Ausrichtung oder eines regionalen Anbieters, der diese Domains verwendet, Bedenken bezüglich einer RBL haben, müssen Sie den Reputationsstatus der dedizierten (verwalteten) IP-Adresse selbst überprüfen.

F5. Wenn SES keine Maßnahmen ergreift, wenn dedizierte IP-Adressen (verwaltet) in einer anderen RBL als Spamhus aufgeführt werden, warum sollte ich sie verwenden?

Dedizierte IP-Adressen (verwaltet) werden im Sinne der auto-scaling verwaltet, indem IP-Adressen auf der Grundlage des Datenverkehrs hinzugefügt und entfernt werden. Außerdem sparen Sie Zeit bei der Aufwärmverwaltung pro Internetdienstanbieter. So verfolgt ein verwalteter Pool anhand von historischen Sendemustern, wie viele E-Mails über jede IP-Adresse versendet werden können. Weitere Vorteile finden Sie in. the section called “Vorteile und Funktionen”

F6. Wie kann ich dedizierte IP-Adressen (verwaltet) nachverfolgen, die für mein Konto geleast wurden?

Sie können einen SES-Konfigurationssatz mit einem Ziel für die Veröffentlichung von Ereignissen verwenden, das entweder für ein Amazon Data Firehose- oder ein Amazon SNS SNS-Thema definiert ist. SES-Liefererereignisse enthalten das Tag. `ses:outgoing-ip` Wenn also eine E-Mail aufgrund der Reputation einer dedizierten IP-Adresse (verwaltet) zurückgewiesen wurde, finden Sie die betreffende dedizierte IP-Adresse (verwaltet) im Tag des Bounce-Ereignisses. `ses:outgoing-ip`

Amazon SES Versandprüfungsprozess FAQs

Wir überwachen über Amazon SES gesendeten E-Mails, um sicherzustellen, dass der Service nicht für die Zustellung schädlicher, unerwünschter oder minderwertiger E-Mails genutzt wird. Wenn wir feststellen, dass ein Benutzer Inhalte sendet, die in eine dieser Kategorien fallen, ergreifen wir für das betreffende Konto Maßnahmen. Wir bezeichnen diesen Prozess als unser Sendeprüfverfahren.

In vielen Fällen, wenn wir ein Problem mit einem Konto erkennen, legen wir eine Prüfung für das betreffende Konto fest. In anderen Fällen unterbrechen wir die Fähigkeit des Kontos, E-Mails zu senden. Wir ergreifen diese Maßnahmen, um den Ruf der einzelnen Konten als Absender zu schützen und um zu verhindern, dass bei anderen SES-Benutzern Serviceunterbrechungen und Probleme mit der Zustellbarkeit auftreten.

Inhalt

- Konto wird geprüft – Häufig gestellte Fragen
- Sendeunterbrechung – Häufig gestellte Fragen
- Unzustellbarkeit – Häufig gestellte Fragen

- Beschwerden – Häufig gestellte Fragen
- Pseudo-E-Mail-Adressen für Spam – Häufig gestellte Fragen
- Manuelle Überprüfung – Häufig gestellte Fragen

Konto wird geprüft – Häufig gestellte Fragen

F1. Ich habe eine Meldung erhalten, die besagt, dass mein Konto geprüft wird. Was bedeutet das?

Wir haben ein Problem mit der E-Mail festgestellt, die Sie von Ihrem Konto gesendet haben, und geben Ihnen Zeit, das Problem zu beheben. Sie können weiterhin E-Mails wie gehabt versenden, sollten jedoch auch das Problem beheben, das zur Festlegung einer Prüfung für Ihr Konto geführt hat. Wenn Sie das Problem vor Ablauf des Überprüfungszeitraums nicht beheben, unterbrechen wir möglicherweise Ihre Fähigkeit, weitere E-Mails zu senden.

F2. Werde ich immer benachrichtigt, wenn eine Prüfung für mein Konto festgelegt ist?

Ja. Sie erhalten eine Benachrichtigung unter der E-Mail-Adresse, die mit Ihrem AWS -Konto verknüpft ist.

F3. Warum wurde ich nicht darüber benachrichtigt, dass mein Konto geprüft wird?

Wenn Ihr Konto überprüft wird, senden wir automatisch eine Benachrichtigung an die mit Ihrem AWS Konto verknüpfte E-Mail-Adresse. Diese E-Mail-Adresse haben Sie bei der Erstellung Ihres AWS Kontos angegeben. In einigen Fällen kann sich diese E-Mail-Adresse von der unterscheiden, die Sie zum Senden von E-Mails mit SES verwenden.

Wir empfehlen, dass Sie Ihre Zuverlässigkeit als Absender überwachen, indem Sie regelmäßig auf das Reputation Dashboard zugreifen. Sie können auch automatische Alarme in Amazon einrichten CloudWatch. Mithilfe dieser Alarme erhalten Sie eine Benachrichtigung, wenn Ihre Zuverlässigkeitsmetriken bestimmte Grenzwerte überschreiten. Sie können Amazon auch so konfigurieren CloudWatch , dass es Sie auf andere Weise kontaktiert, z. B. indem Sie eine Textnachricht an Ihr Handy senden.

F4. Wird sich die Tatsache, dass mein SES-Konto überprüft wird, auf meine Nutzung anderer AWS Dienste auswirken?

Sie können weiterhin andere AWS Dienste nutzen, solange Ihr SES-Konto überprüft wird. Wenn Sie jedoch eine Erhöhung des Servicekontingents für einen anderen AWS Service beantragen, der

ausgehende Nachrichten sendet (z. B. Amazon SNS), kann diese Anfrage abgelehnt werden, bis der Überprüfungszeitraum für Ihr SES-Konto aufgehoben wird.

F5. Was soll ich tun, wenn mein Konto geprüft wird?

Sie sollten Folgendes tun:

- Wenn Ihre Situation es zulässt, stoppen Sie den Versand von E-Mails, bis Sie das Problem behoben haben. Sie können weiterhin E-Mails versenden, während Ihr Konto geprüft wird. Wenn Sie jedoch weiterhin E-Mails senden, ohne Änderungen vorzunehmen, können Sie das Problem versehentlich verschlimmern.
- In der E-Mail, die Sie von uns erhalten haben, finden Sie eine Zusammenfassung des Problems.
- Untersuchen Sie Ihren Sendeprozess, um festzustellen, welcher Aspekt dabei das Problem speziell ausgelöst hat.
- Nachdem Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie in Ihrer Nachricht detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt.
- Stellen Sie sicher, dass Sie uns alle Informationen, die wir ausdrücklich anfordern, zur Verfügung stellen. Wir benötigen diese Informationen, um Ihren Fall zu bewerten.

F6. Wie kann ich eine Überprüfung beantragen?

Sie können beantragen, dass wir unsere Entscheidung, Ihr Konto zu überprüfen, überprüfen. Um eine Bewertung anzufordern, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben.

Machen Sie in Ihre Anfrage die folgenden Angaben:

- Informationen zur Ursache des Ereignisses, das zur Festlegung einer Prüfung für Ihr Konto geführt hat.
- Eine Liste der Änderungen, die Sie vorgenommen haben, um das Problem zu beheben. Geben Sie nur die Schritte an, die Sie bereits implementiert haben, keine Schritte, die Sie in Zukunft implementieren möchten.
- Informationen darüber, wie diese Änderungen verhindern, dass dasselbe Problem in Zukunft erneut auftritt.

Abhängig von der Art des Ereignisses, das zur Festlegung einer Prüfung für Ihr Konto geführt hat, benötigen wir möglicherweise weitere Informationen. Eine Liste der Informationen, die Sie in Ihrer Anfrage bereitstellen sollten, finden Sie in den häufig gestellten Fragen im passenden Thema zu Ihrem Problem.

F7. Was soll ich tun, wenn meine Überprüfungsanfrage nicht akzeptiert wird?

Wir beantworten Ihre Anfrage mit Informationen, warum wir ihr nicht stattgegeben haben. In einigen Fällen können Sie eine weitere Anfrage senden, wenn Sie nachweisen können, dass Sie das Problem behoben haben und Ihre Änderungen verhindern, dass das Problem zukünftig erneut auftritt.

F8. Können Sie mir helfen, das Problem zu diagnostizieren?

In der Regel können wir Ihnen nur eine allgemeine Übersicht über Ihr Problem geben (etwa dass ein Problem mit unzustellbaren Nachrichten vorliegt). Die Ursache muss von Ihnen selbst untersucht werden.

F9. Wie erfahre ich, ob mein Konto nun nicht mehr geprüft wird?

Das Reputation Dashboard enthält Informationen zum aktuellen Status Ihres Kontos. Weitere Informationen finden Sie unter Verwenden des Reputation Dashboards zum Nachverfolgen von Unzustellbarkeits- und Beschwerdequoten.

F10. Wird für mein Konto jedes Mal, wenn ein Problem auftritt, eine Prüfung festgelegt?

Nein. In einigen Fällen unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu versenden, ohne zuerst eine Prüfung für Ihr Konto festzulegen. Beispiel:

- Wenn das Problem schwerwiegend ist.
- Wenn für Ihr Konto zuvor bereits mehrmals aufgrund desselben Problems eine Prüfung festgelegt wurde. Daher ist es wichtig, das zugrunde liegende Problem anzugehen und nicht nur den jeweiligen Vorfall zu beheben, der zur Festlegung einer Prüfung für Ihr Konto führte. Wenn beispielsweise eine bestimmte Kampagne uns dazu bewegt hat, für Ihr Konto eine Prüfung festzulegen, müssen Sie mehr tun, als einfach nur die Kampagne zu stoppen. Sie sollten bestimmen, welche Eigenschaften der Kampagne problematisch waren, und sicherstellen, dass Sie über entsprechende Prozesse verfügen, damit bei Ihren zukünftigen Kampagnen nicht dasselbe Problem auftritt.

In beiden Fällen senden wir Ihnen automatisch eine Benachrichtigung, wenn wir die Fähigkeit Ihres Kontos zum Senden von E-Mails unterbrechen.

F11. Was passiert, wenn ich meine Korrekturen erst kurz vor Ende des Überprüfungszeitraums durchführe?

Melden Sie sich im an AWS-Managementkonsole und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Teilen Sie uns in Ihrer Antwort auf den Fall mit, dass Sie das Problem gelöst haben.

F12. Kann ich Hilfe von meinem AWS Vertreter oder vom Premium-Support Support?

Wenn Sie bereits mit einem AWS Kundenbetreuer zusammenarbeiten, werden wir ihn oder sie automatisch kontaktieren, sobald Ihr Konto geprüft wird. Ihr Kundenbetreuer kann Ihnen zusätzliche Informationen bereitstellen, die Ihnen helfen, das Problem besser zu verstehen. Wenn Sie Premium Support verwenden, sollten Sie sich auch an das Team wenden, um Hilfe zu erhalten.

Sendeunterbrechung – Häufig gestellte Fragen

F1. Ich erhalte eine Meldung, die besagt, dass die Fähigkeit meines Kontos zum Versenden von E-Mails unterbrochen ist. Was bedeutet das?

Wir haben die Fähigkeit Ihres Kontos zum Versenden von E-Mails aufgrund eines schwerwiegenden Problems mit den von Ihnen gesendeten E-Mails unterbrochen. In den meisten Fällen pausieren wir Konten aus einem der folgenden Gründe:

- Wir legten zuvor eine Prüfung für Ihr Konto fest. Die Probleme, die dazu führten, dass wir eine Prüfung für Ihr Konto festgelegt haben, wurden vor Ablauf des Überprüfungszeitraums nicht korrigiert. Wir haben daher die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrochen.
- Wir haben bereits mehrmals für dasselbe Problem eine Prüfung für Ihr Konto festgelegt.
- Von Ihrem Konto wurden E-Mails gesendet, die gegen die AWS -Servicebedingungen verstießen. Wenn diese Verstöße schwerwiegend sind, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu versenden, ohne zuerst eine Prüfung für Ihr Konto festzulegen.

F2. Werde ich immer benachrichtigt, wenn die Fähigkeit meines Kontos zum Versenden von E-Mails unterbrochen wird?

Ja. Sie erhalten eine Benachrichtigung unter der E-Mail-Adresse, die mit Ihrem AWS -Konto verknüpft ist.

F3. Die Fähigkeit meines Kontos, E-Mails zu versenden, wurde unterbrochen. Warum habe ich keine Benachrichtigung erhalten?

Wenn wir die Fähigkeit eines Kontos zum Versenden von E-Mails unterbrechen, senden wir automatisch eine Benachrichtigung an die E-Mail-Adresse, die mit diesem Konto verknüpft ist.

> **Note**
>
> Wenn Sie Ihr AWS Konto erstellen, müssen Sie eine E-Mail-Adresse angeben. Sie können diese Adresse jederzeit ändern. Weitere Informationen zum Ändern der mit Ihrem AWS Konto verknüpften Adresse finden Sie im AWS Fakturierung und Kostenmanagement Benutzerhandbuch unter Ein AWS Konto verwalten.

Sie können Amazon verwenden CloudWatch , um Alarme zu erstellen, die Sie informieren, wenn Ihre Absprungs- und Beschwerdequoten zu hoch sind. Das Erstellen eines Alarms ist eine gute Möglichkeit, eine frühe Warnung vor Faktoren zu erhalten, die dazu führen können, dass wir die Fähigkeit Ihres Konto zum Senden von E-Mails vorübergehend unterbrechen können. Es gibt jedoch andere Faktoren als Unzustellbarkeitsnachrichten und Beschwerden, die dazu führen können, dass wir Ihre Fähigkeit zum Senden von E-Mails vorübergehend unterbrechen. Weitere Informationen zum Erstellen von Alarmen in finden Sie CloudWatch unterErstellen von Alarmen zur Reputationsüberwachung mit CloudWatch.

Sie können auch das Konto-Dashboard verwenden, um den aktuellen Status Ihres Kontos zu bestimmen. Beispiel: Wenn die Fähigkeit Ihres Kontos, E-Mails zu senden, derzeit unterbrochen ist, zeigt der Abschnitt Account status (Kontostatus) des Konto-Dashboards den Status Paused (Unterbrochen) an. Wenn Ihr Konto E-Mails normal senden kann, zeigt es den Status Healthy (Stabil) an.

Schließlich können Sie anhand der Option AWS Health Dashboard (PHD) unter https://phd.aws.amazon.com/feststellen, ob die E-Mail-Funktion Ihres Kontos derzeit unterbrochen ist. Wenn wir die Fähigkeit, E-Mails zu senden, vorübergehend unterbrechen, fügen wir automatisch

ein Ereignis SES sending paused (SES-Senden unterbrochen) dem Abschnitt Event log (Ereignisprotokoll) der PHD hinzu. Das Ereignis SES sending paused (SES-Senden unterbrochen) hat immer den Status Closed (Geschlossen), unabhängig davon, ob die Fähigkeit des Kontos zum Versenden von E-Mails derzeit ausgesetzt ist. Das Ereignisprotokoll enthält auch eine Kopie der E-Mail, die wir an die mit Ihrem AWS Konto verknüpfte E-Mail-Adresse gesendet haben, als die Versandpause eintrat.

Sie können CloudWatch damit Alarme erstellen, die Sie benachrichtigen, wenn neue Ereignisse in Ihrem Personal Health Dashboard erscheinen. Weitere Informationen finden Sie unter AWS Health Ereignisse anhand von CloudWatch Ereignissen überwachen im AWS Health Benutzerhandbuch.

F4. Die Fähigkeit meines Kontos, E-Mails zu versenden, wurde unterbrochen. Beeinträchtigt dies meine Fähigkeit, andere AWS Dienste zu nutzen?

Sie können weiterhin andere AWS Dienste nutzen, solange die Fähigkeit Ihres Kontos, E-Mails zu senden, unterbrochen ist. Wenn Sie jedoch eine Erhöhung des Servicekontingents für einen anderen AWS -Service anfordern, der ausgehende Kommunikation sendet (z. B. Amazon SNS), lehnen wir diesen Antrag so lange möglicherweise ab, bis Ihr Konto wieder E-Mails senden kann.

F5. Was soll ich tun, wenn für mein Konto die Fähigkeit zum Versenden von E-Mails unterbrochen ist?

Sie sollten Folgendes tun:

- In der E-Mail, die Sie von uns erhalten haben, finden Sie eine Zusammenfassung des Problems.
- Untersuchen Sie Ihren Sendeprozess, um festzustellen, welcher Aspekt dabei das Problem speziell ausgelöst hat.
- Nachdem Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie in Ihrer Nachricht detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt.
- Stellen Sie sicher, dass Sie uns alle Informationen, die wir ausdrücklich anfordern, zur Verfügung stellen. Wir benötigen diese Informationen, um Ihren Fall zu bewerten.

F6. Was ist eine Überprüfung?

Sie können anfordern, dass wir unsere Entscheidung überprüfen, eine Prüfung für Ihr Konto festzulegen. Die nachstehende Frage enthält weitere Informationen zum Beantragen einer Überprüfung.

F7. Wie kann ich eine Überprüfung beantragen?

Um eine Bewertung anzufordern, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben.

Machen Sie in Ihre Anfrage die folgenden Angaben:

- Informationen über die Ursache des Problems.
- Eine Liste der Änderungen, die Sie vorgenommen haben, um das Problem zu beheben. Geben Sie nur die Schritte an, die Sie bereits implementiert haben, keine Schritte, die Sie in Zukunft implementieren möchten.
- Informationen darüber, wie diese Änderungen verhindern, dass dasselbe Problem zukünftig erneut auftritt.

Abhängig von der Art des Ereignisses, das zur Unterbrechung der Fähigkeit zum Versenden von E-Mails für Ihr Konto geführt hat, benötigen wir möglicherweise weitere Informationen. Eine Liste der Informationen, die Sie in Ihrer Anfrage bereitstellen sollten, finden Sie in den häufig gestellten Fragen im passenden Thema zu Ihrem Problem.

F8. Was soll ich tun, wenn meine Anfrage nicht akzeptiert wird?

Wir beantworten Ihre Anfrage mit Informationen, warum wir ihr nicht stattgegeben haben. In einigen Fällen können Sie eine weitere Anfrage senden, wenn Sie nachweisen können, dass Sie das Problem behoben haben und Ihre Änderungen verhindern, dass das Problem zukünftig erneut auftritt.

F9. Können Sie mir helfen, das Problem zu diagnostizieren?

In der Regel können wir Ihnen nur eine allgemeine Übersicht über Ihr Problem geben (etwa dass ein Problem mit unzustellbaren Nachrichten vorliegt). Es liegt in Ihrer Verantwortung, das Problem zu beheben.

F10. Wie kann ich wissen, ob die Fähigkeit meines Kontos, E-Mails zu versenden, wiederhergestellt wurde?

Das Reputation Dashboard enthält Informationen zum aktuellen Status Ihres Kontos. Weitere Informationen finden Sie unter Verwenden des Reputation Dashboards zum Nachverfolgen von Unzustellbarkeits- und Beschwerdequoten.

F11. Kann ich Hilfe von meinem AWS Vertreter oder vom Premium-Support Support?

Wenn du bereits mit einem AWS Kundenbetreuer zusammenarbeitest, werden wir ihn oder sie automatisch kontaktieren, wenn wir den E-Mail-Versand deines Accounts unterbrechen. Ihr Kundenbetreuer kann Ihnen zusätzliche Informationen bereitstellen, die Ihnen helfen, das Problem besser zu verstehen. Wenn Sie Premium Support verwenden, sollten Sie sich auch an das Team wenden, um Hilfe zu erhalten.

Unzustellbarkeit – Häufig gestellte Fragen

F1. Warum interessieren Sie meine unzustellbaren Nachrichten?

Hohe Unzustellbarkeitsraten werden häufig von Entitäten wie E-Mail-Anbietern und Anti-Spam-Organisationen dazu herangezogen, um Absender zu erkennen, die schlechte E-Mail-Versandpraktiken anwenden. Hohe Unzustellbarkeitsraten können dazu führen, dass E-Mails nicht an den Posteingang, sondern an den Spam-Ordner gesendet werden.

F2. Was soll ich tun, wenn mir in einer Benachrichtigung mitgeteilt wird, dass mein Konto geprüft wird oder dass für mich das Senden aufgrund der Unzustellbarkeitsquote meines Kontos unterbrochen wurde?

Identifizieren Sie die Ursache des Problems und korrigieren Sie es. Nachdem Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie in Ihrer Nachricht detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt. Schließen Sie außerdem die folgenden Informationen ein:

- Die Methode, die Sie zur Nachverfolgung Ihrer unzustellbaren Nachrichten verwenden
- Die Art und Weise, wie Sie sicherstellen, dass die E-Mail-Adressen neuer Empfänger gültig sind, bevor Nachrichten an sie gesendet werden. Beispielsweise, welche der aufgeführten

Empfehlungen befolgen Sie in F11. Was kann ich tun, um die Zahl unzustellbarer Nachrichten zu minimieren?

F3. Welche Arten von unzustellbaren Nachrichten zählen zu meiner Unzustellbarkeitsquote?

Ihre Unzustellbarkeitsquote umfasst nur permanent unzustellbare Nachrichten an Domänen, die Sie nicht überprüft haben. Permanente Unzustellbarkeit liegt vor, wenn dauerhafte Fehler bei der Übermittlung auftreten, wie etwa "Adresse ist nicht vorhanden". Temporäre und vorübergehende Fehler wie "Postfach voll" oder Unzustellbarkeit aufgrund von blockierten IP-Adressen werden bei Ihrer Unzustellbarkeitsquote nicht berücksichtigt.

F4. Legen Sie Unzustellbarkeitsquoten offen, die dazu führen könnten, dass eine Prüfung für mein Konto festgelegt wird oder für mich das Senden unterbrochen wird?

Sie erzielen die besten Ergebnisse mit einer Unzustellbarkeitsquote von unter 2 %. Höhere Unzustellbarkeitsquoten können den Versand Ihrer E-Mails beeinflussen.

Wenn Ihre Unzustellbarkeitsquote mehr als 5 % beträgt, legen wir für Ihr Konto eine Prüfung fest. Wenn Ihre Unzustellbarkeitsquote 10 % oder höher ist, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos zum Versenden weiterer E-Mails, bis Sie das Problem behoben haben, das zu der hohen Unzustellbarkeitsquote führte.

F5. Über welche Zeitspanne hinweg wird meine Unzustellbarkeitsquote berechnet?

Wir berechnen die Unzustellbarkeitsquote nicht basierend auf einem festen Zeitraum, da verschiedene Sender in unterschiedlichem Tempo Nachrichten senden. Stattdessen wird eine repräsentative Menge herangezogen. Dies ist eine Anzahl von E-Mails, die Ihr typisches Sendeverhalten repräsentiert. Um sowohl Sendern großer Mengen als auch Sendern kleinerer Mengen gerecht zu werden, ist die repräsentative Menge für jeden Benutzer unterschiedlich und ändert sich, wenn sich das Sendemuster des Benutzers ändert.

F6. Kann ich anhand der Informationen aus der SES-Konsole oder der GetSendStatistics API meine eigene Absprungrate berechnen?

Nein. Die Unzustellbarkeitsquote wird anhand der repräsentativen Menge berechnet (siehe F5. Über welche Zeitspanne hinweg wird meine Unzustellbarkeitsquote berechnet?). Abhängig von Ihrer Senderate kann Ihre Absprungrate weiter zurückreichen als die SES-Konsole oder `GetSendStatistics` die Abrufrate. Außerdem werden bei der Berechnung Ihrer

Unzustellbarkeitsquote nur E-Mails an nicht verifizierte Domänen berücksichtigt. Wenn Sie jedoch Ihre Unzustellbarkeitsquoten regelmäßig mit diesen Methoden überwachen, sollten Sie doch einen guten Indikator haben, der Ihnen helfen kann, Probleme zu erkennen, bevor sie ein Level erreichen, das zur Festlegung einer Prüfung für Ihr Konto oder zur Unterbrechung der Fähigkeit Ihres Kontos zum Versenden von E-Mails führen kann.

F7. Wie kann ich herausfinden, an welche E-Mail-Adressen Nachrichten nicht zugestellt werden konnten?

Prüfen Sie die Bounce-Benachrichtigungen, die SES Ihnen sendet. Die E-Mail-Adresse, an die SES die Benachrichtigungen weiterleitet, hängt davon ab, wie Sie die ursprünglichen Nachrichten gesendet haben, wie unter beschrieben. Verwenden von Benachrichtigungen für den Amazon-SES-E-Mail-Empfang Sie können auch Unzustellbare Benachrichtigungen über Amazon Simple Notification Service (Amazon SNS) einrichten, wie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES beschrieben. Beachten Sie, dass durch das einfache Entfernen der unzustellbaren Adressen aus der Liste ohne zusätzliche Untersuchung das zugrunde liegende Problem möglicherweise nicht gelöst wird. Informationen dazu, was Sie tun können, um die Zahl nicht zustellbarer Nachrichten zu reduzieren, finden Sie unter F11. Was kann ich tun, um die Zahl unzustellbarer Nachrichten zu minimieren?.

F8. Wenn ich meine unzustellbaren Nachrichten nicht überwacht habe, können Sie mir eine Liste der Adressen senden, die unzustellbar waren?

Nein, wir können keine vollständige Liste der Adressen bereitstellen, die unzustellbar waren. Sie sind verantwortlich für die Überwachung und die Einleitung von Maßnahmen bei Unzustellbarkeitsereignissen für Ihr Konto.

F9. Wie soll ich mit unzustellbaren Nachrichten umgehen?

Sie müssen Adressen, an die Nachrichten nicht zugestellt werden konnten, aus Ihrer Mailing-Liste entfernen und den Versand von E-Mails an diese Adressen sofort beenden. Wenn Sie geringe Mengen versenden, kann es unter Umständen ausreichen, einfach die Unzustellbarkeit per E-Mail zu überwachen und Adressen mit fehlgeschlagener Zustellung manuell aus Ihrer Mailing-Liste zu entfernen. Wenn Sie größere Mengen versenden, sollten Sie diesen Prozess automatisieren, entweder durch programmgesteuerte Verarbeitung des Postfachs, in dem nicht zugestellte Nachrichten eingehen, oder durch Einrichten von Unzustellbarkeitsbenachrichtigungen über Amazon SNS. Weitere Informationen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.

F10. Ist es möglich, dass meine E-Mails nicht zugestellt werden können, weil ich die Grenze meines Sendekontingents erreicht habe?

Nein. Unzustellbarkeiten stehen nicht im Zusammenhang Sendekontingenten. Wenn Sie versuchen, Ihr Versandkontingent zu überschreiten, erhalten Sie beim Versuch, eine E-Mail zu senden, eine Fehlermeldung von der SES-API oder der SMTP-Schnittstelle.

F11. Was kann ich tun, um die Zahl unzustellbarer Nachrichten zu minimieren?

Stellen Sie zunächst sicher, dass Sie wissen, welche Nachrichten nicht zugestellt werden konnten (siehe F7. Wie kann ich herausfinden, an welche E-Mail-Adressen Nachrichten nicht zugestellt werden konnten?). Befolgen Sie dann diese Richtlinien:

- Kaufen oder mieten Sie keine E-Mail-Adressen und geben Sie keine E-Mail-Adressen weiter. Senden Sie E-Mails nur an Empfänger, die E-Mails von Ihnen explizit angefordert haben.
- Entfernen Sie Adressen, an die Nachrichten nicht zugestellt werden konnten, aus Ihrer Liste.
- Bitten Sie Benutzer, ihre E-Mail-Adressen auf Webformularen zwei Mal anzugeben, und stellen Sie sicher, dass beide Adressen übereinstimmen, bevor das Formular gesendet werden kann.
- Verwenden Sie bei der Registrierung neuer Benutzer ein Double-Opt-in-Verfahren für die doppelte Anmeldung. Das bedeutet Folgendes: Wenn sich neue Benutzer registrieren, senden Sie Ihnen eine Bestätigungs-E-Mail, auf die sie klicken müssen, bevor sie weitere E-Mails erhalten. Dadurch wird verhindert, dass Personen andere Personen registrieren oder Anmeldungen versehentlich stattfinden.
- Wenn Sie Nachrichten an Adressen senden müssen, an die Sie in letzter Zeit keine Nachrichten gesendet haben (und Sie daher nicht sicher sein können, dass die Adressen noch gültig sind), tun Sie dies nur mit einem kleinen Teil der gesamten Sendung. Weitere Informationen finden Sie in unserem Blog-Beitrag Never send to old addresses, but what if you have to?.
- Stellen Sie sicher, dass Sie Anmeldungen nicht so strukturieren, dass Personen dazu ermutigt werden, fiktive Adressen zu verwenden. Bieten Sie beispielsweise keinen Mehrwert oder Leistungen, bevor die Empfänger ihre Adressen bestätigt haben.
- Wenn Sie eine Funktion wie "E-Mail an einen Freund senden" bieten, verwenden Sie CAPTCHA oder einen ähnlichen Mechanismus, um eine automatisierte Nutzung der Funktion zu verhindern, und lassen Sie das Einfügen beliebiger Inhalte nicht zu.
- Wenn Sie SES für Systembenachrichtigungen verwenden, stellen Sie sicher, dass Sie die Benachrichtigungen an echte Adressen senden, die E-Mails empfangen können. Ziehen Sie außerdem in Betracht, Benachrichtigungen, die Sie nicht benötigen, zu deaktivieren.

- Wenn Sie ein neues System testen, stellen Sie sicher, dass Sie entweder an echte Adressen senden, die E-Mails empfangen können, oder dass Sie den SES-Postfachsimulator verwenden. Weitere Informationen finden Sie unter Manuelles Verwenden des Postfachsimulators.

Beschwerden – Häufig gestellte Fragen

F1. Was ist eine Beschwerde?

Eine Beschwerde liegt vor, wenn Empfänger melden, dass sie eine E-Mail nicht erhalten möchten. Möglicherweise haben sie in ihrem E-Mail-Client auf die Schaltfläche „Spam melden“ geklickt, sich bei ihrem E-Mail-Anbieter beschwert, SES direkt oder auf andere Weise benachrichtigt. Dieses Thema enthält allgemeine Informationen zu Beschwerden. Wenn Ihre Benachrichtigung spezifische Informationen über die Quelle der Beschwerden enthält, lesen Sie auch das entsprechende Thema:

- Häufig gestellte Fragen zu SES-Beschwerden über Feedback-Schleifen
- Häufig gestellte Fragen zu SES-Beschwerden direkt von Empfängern
- Häufig gestellte Fragen zu SES-Beschwerden über E-Mail-Anbieter

F2. Warum interessieren Sie meine Beschwerden?

Hohe Beschwerdequoten dienen Organisationen wie E-Mail-Dienstanbietern und Anti-Spam-Organisationen häufig als Indikatoren dafür, dass ein Sender E-Mails an Empfänger sendet, die sich nicht speziell für den Erhalt von E-Mails angemeldet haben, oder dass der Sender Inhalte sendet, die sich von der Art Inhalte unterscheiden, für die sich die Empfänger angemeldet haben.

F3. Was soll ich tun, wenn mir in einer Benachrichtigung mitgeteilt wird, dass mein Konto geprüft wird, oder dass für mich das Senden aufgrund eines Problems mit Beschwerden unterbrochen wird?

Überprüfen Sie Ihren Listenakquisitionsprozess und den Inhalt Ihrer E-Mails, um zu verstehen, warum die Empfänger Ihre E-Mails möglicherweise nicht erhalten möchten. Identifizieren Sie die Ursache des Problems und korrigieren Sie es. Nachdem Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie in Ihrer Nachricht detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt.

F4. Was kann ich tun, um Beschwerden zu minimieren?

Stellen Sie zunächst sicher, dass Sie die Beschwerden im Auge behalten, über die SES Sie benachrichtigen kann. Dabei handelt es sich um Beschwerden, die SES über Feedback-Schleifen erhält (siehe Häufig gestellte Fragen zu SES-Beschwerden über Feedback-Schleifen). Befolgen Sie dann diese Richtlinien:

- Kaufen oder mieten Sie keine E-Mail-Adressen und geben Sie keine E-Mail-Adressen weiter. Verwenden Sie nur E-Mail-Adressen, die Ihre E-Mails explizit angefordert haben.
- Verwenden Sie bei der Registrierung neuer Benutzer ein Double-Opt-in-Verfahren für die doppelte Anmeldung. Das bedeutet Folgendes: Wenn sich neue Benutzer registrieren, senden Sie Ihnen eine Bestätigungs-E-Mail, auf die sie klicken müssen, bevor sie weitere E-Mails erhalten. Dadurch wird verhindert, dass Personen andere Personen registrieren oder Anmeldungen versehentlich stattfinden.
- Überwachen Sie die Interaktionen mit den von Ihnen gesendeten E-Mails und senden Sie keine E-Mails mehr an Empfänger, die Ihre Nachrichten nicht öffnen und nicht darauf klicken.
- Wenn sich neue Benutzer anmelden, machen Sie deutlich, welche Art von E-Mail sie von Ihnen erhalten werden, und stellen Sie sicher, dass Sie ihnen nur die Art von E-Mails senden, für die sie sich angemeldet haben. Senden Sie beispielsweise Benutzern, die sich für aktuelle Nachrichten angemeldet haben, keine Werbung.
- Stellen Sie sicher, dass Ihre E-Mails gut formatiert sind und professionell aussehen.
- Sorgen Sie dafür, dass Ihre E-Mails klar erkennbar von Ihnen stammen und nicht mit etwas anderem verwechselt werden können.
- Bieten Sie Ihren Benutzern eine offensichtliche und einfache Option, das Abonnement für Ihre E-Mails zu kündigen.

Häufig gestellte Fragen zu SES-Beschwerden über Feedback-Schleifen

Dieses Thema enthält Informationen zu Beschwerden, die SES von E-Mail-Anbietern im Rahmen von Feedback-Schleifen erhält. Allgemeine Informationen, die für alle Arten von Beschwerden gelten, finden Sie unter Beschwerden – Häufig gestellte Fragen.

F1. Wie wird diese Art Beschwerde gemeldet?

Die meisten E-Mail-Client-Programme bieten eine Schaltfläche wie „Als Spam markieren“ o. Ä., über die die Nachricht in einen Spam-Ordner verschoben und an den E-Mail-Anbieter weitergeleitet

wird. Darüber hinaus unterhalten die meisten E-Mail-Anbieter eine Missbrauchsadresse (z. B. missbrauch@example.com), an die Benutzer unerwünschte E-Mails weiterleiten und den Anbieter auffordern können, entsprechende Maßnahmen zu ergreifen, um solche E-Mails zu verhindern. Wenn SES eine Feedback-Schleife (FBL) mit dem E-Mail-Anbieter eingerichtet hat, wird die Beschwerde an SES zurückgesendet.

> **Note**
>
> SES legt automatisch den Feedback-ID-Header fest, wenn Sie Nachrichten senden, sodass Postfachanbieter die Möglichkeit haben, Zustellungsstatistiken wie Beschwerde- und Spam-Raten zu aggregieren und Ihnen zur Verfügung zu stellen. Der von SES bereitgestellte Feedback-ID-Header-Wert setzt sich wie folgt zusammen:
>
> - `FeedBackId:((SESInternalID):(AmazonSES))`, wobei:
>   - SESInternalID ist die Kennung, die von SES für die Erfassung von Beschwerdeinformationen verwendet wird.
>   - AmazonSES ist ein statisches Tag, das SES als sendende Plattform identifiziert.
>
> Optional können Sie zusätzlich zum standardmäßigen Feedback-ID-Header-Wert, den SES bereitstellt, auch Ihr eigenes benutzerdefiniertes Feedback IDs (bis zu zwei) mithilfe der `ses:feedback-id-b` Nachrichten-Tags `ses:feedback-id-a` und -Message-Tags angeben, siehe. the section called “Detailliertes Feedback für E-Mail-Kampagnen”

F2. Sind diese Beschwerden in der Statistik zur Beschwerdequote enthalten, die in der SES-Konsole angezeigt und von der API zurückgesendet wird? GetSendStatistics

Ja. In der Statistik der Beschwerdequote sind jedoch keine Beschwerden von E-Mail-Anbietern enthalten, die SES kein Feedback geben. Die Beschwerdequote von Domänen, die Feedback bereitstellen, ist wahrscheinlich auch für den Rest Ihrer E-Mail-Sendungen repräsentativ.

F3. Wie kann ich über diese Beschwerden informiert werden?

Sie können per E-Mail oder über Amazon-SNS-Benachrichtigungen informiert werden. Anweisungen zur Einrichtung finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.

F4. Was soll ich tun, wenn ich eine Beschwerdebenachrichtigung per E-Mail oder über Amazon SNS erhalte?

Zuerst müssen Sie die Adressen, die Beschwerden generierten, aus Ihrer Mailing-Liste entfernen und den Versand von E-Mails an diese Adressen sofort beenden. Senden Sie nicht einmal eine E-Mail, um zu bestätigen, dass Sie die Aufforderung zur Abmeldung erhalten haben. Erwägen Sie, diesen Prozess zu automatisieren, entweder durch programmgesteuerte Verarbeitung des Postfachs, in dem Beschwerden eingehen, oder durch Einrichten von Beschwerdebenachrichtigungen über Amazon SNS. Weitere Informationen finden Sie unter Einrichten von Ereignisbenachrichtigungen für Amazon SES.

Anschließend sollten Sie Ihren Versand genau überprüfen, um zu ermitteln, warum Ihre Empfänger die von Ihnen gesendeten E-Mails nicht wünschen, und dann das zugrunde liegende Problem beheben. Für jede Person, die sich beschwert, gibt es möglicherweise Dutzende, die ebenfalls keinen Wert auf Ihre E-Mail legen, sich aber nicht beschwerten (oder nicht dazu in der Lage waren). Wenn Sie lediglich die Empfänger entfernen, die sich tatsächlich beschweren, beheben Sie nicht das zugrunde liegende Problem.

F5. Geben Sie die Beschwerdequoten von SES an, die dazu führen könnten, dass mein Konto überprüft wird oder die dazu führen könnten, dass die Fähigkeit meines Kontos, E-Mails zu senden, unterbrochen wird?

Sie erzielen die besten Ergebnisse mit einer Beschwerdequote von unter 0,1 %. Höhere Beschwerdequoten können den Versand Ihrer E-Mails beeinflussen.

Wenn Ihre Beschwerdenquote mehr als 0,1 % beträgt, legen wir für Ihr Konto eine Prüfung fest. Wenn Ihre Beschwerdenquote 0,5 % oder höher ist, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos zum Verwenden weiterer E-Mails, bis Sie das Problem behoben haben, das zu der hohen Beschwerdequote führte.

F6. Über welche Zeitspanne hinweg wird meine Beschwerdequote berechnet?

Wir berechnen die Beschwerdequote nicht basierend auf einem festen Zeitraum, da verschiedene Sender in unterschiedlichem Tempo Nachrichten senden. Stattdessen wird eine repräsentative Menge herangezogen. Dies ist eine Anzahl von E-Mails, die Ihr typisches Sendeverhalten repräsentiert. Um sowohl Sendern großer Mengen als auch Sendern kleinerer Mengen gerecht zu werden, ist die repräsentative Menge für jeden Benutzer unterschiedlich und ändert sich, wenn sich das Sendemuster des Benutzers ändert. Darüber hinaus wird die Beschwerdequote nicht basierend auf jeder E-Mail berechnet. Stattdessen wird sie als Prozentsatz der Beschwerden über E-Mails berechnet, die an Domains gesendet wurden, die Feedback zu Beschwerden an SES senden.

F7. Kann ich meine eigene Beschwerdequote anhand von Kennzahlen aus der SES-Konsole oder der GetSendStatistics API berechnen?

Nein. Hierfür gibt es zwei primäre Gründe:

- Die Beschwerdequote wird anhand der repräsentativen Menge berechnet (siehe F6. Über welche Zeitspanne hinweg wird meine Beschwerdequote berechnet?). Abhängig von Ihrer Senderate kann Ihre Beschwerderate weiter in die Vergangenheit zurückreichen, als die SES-Konsole oder die `GetSendStatistics` SES-API abrufen kann. Aus diesem Grund empfehlen wir, dass Sie regelmäßig diese Methoden zur Überwachung der Beschwerdequote für Ihr Konto verwenden. Wenn Sie Ihre Beschwerdequote auf diese Weise überwachen, erhalten Sie die Informationen, die Sie benötigen, um Probleme zu identifizieren, bevor sie Levels erreichen, die Ihre E-Mail-Zustellung beeinträchtigen könnten.
- Bei der Berechnung der Beschwerdequote zählt nicht jede einzelne E-Mail. Die Beschwerderate wird als Prozentsatz der Beschwerden über E-Mails berechnet, die an Domains gesendet werden, die Feedback zu Beschwerden an SES senden.

F8. Wie kann ich herausfinden, von welchen E-Mail-Adressen Beschwerden kamen?

Prüfen Sie die Beschwerdebenachrichtigungen, die SES Ihnen per E-Mail oder Amazon SNS sendet (sieheEinrichten von Ereignisbenachrichtigungen für Amazon SES). Verschiedene E-Mail-Anbieter stellen jedoch unterschiedliche Informationsmengen zur Verfügung, und einige Anbieter unkenntlich machen die E-Mail-Adresse des Empfängers, bevor sie die Beschwerdebenachrichtigung an SES weiterleiten. Damit Sie die E-Mail-Adresse des Empfängers in future finden können, speichern Sie am besten Ihre eigene Zuordnung zwischen einer Kennung und der SES-Nachrichten-ID, die SES Ihnen zurückgibt, wenn es die E-Mail akzeptiert. Beachten Sie, dass SES keine von Ihnen IDs hinzugefügten benutzerdefinierten Nachrichten speichert.

F9. Wenn ich meine Beschwerden nicht überwacht habe, können Sie mir eine Liste der Adressen senden, von denen Beschwerden geschickt wurden?

Leider können wir Ihnen keine umfassende Liste bereitstellen. Sie können jedoch zukünftige Beschwerden per E-Mail oder über Amazon SNS überwachen.

F10. Kann ich eine Beispiel-E-Mail erhalten?

Wir können Ihnen keine Beispiel-E-Mail auf Anfrage senden, aber Sie finden diese Informationen in der Beschwerdebenachrichtigung. Weitere Informationen finden Sie unter F8. Wie kann ich herausfinden, von welchen E-Mail-Adressen Beschwerden kamen?.

Häufig gestellte Fragen zu SES-Beschwerden direkt von Empfängern

Dieses Thema enthält Informationen zu Beschwerden, die SES direkt von Empfängern erhält. Allgemeine Informationen, die für alle Arten von Beschwerden gelten, finden Sie unter Beschwerden – Häufig gestellte Fragen.

F1. Wie wird diese Art Beschwerde gemeldet?

Mehrere Empfänger haben SES wegen Ihrer Post direkt per E-Mail oder auf andere Weise kontaktiert.

F2. Sind diese Beschwerden in der Statistik der Beschwerdequote enthalten, die in der SES-Konsole angezeigt und von der GetSendStatistics API zurückgesendet wird?

Nein. Die Statistik der Beschwerdequote, die Sie über die SES-Konsole oder die `GetSendStatistics` API abrufen, umfasst nur Beschwerden, die SES über Feedback-Loops erhält. Weitere Informationen zu diesen Arten von Beschwerden finden Sie unter Häufig gestellte Fragen zu SES-Beschwerden über Feedback-Schleifen.

F3. Warum wurde ich nicht durch Feedback-Benachrichtigungen per E-Mail oder über Amazon SNS über diese Beschwerden informiert?

Die Weiterleitung von Feedback per E-Mail und Amazon SNS SNS-Benachrichtigungen umfassen nur Beschwerden, die SES über Feedback-Schleifen erhält. Sie erhalten keine Benachrichtigungen für Beschwerden, die Empfänger direkt bei SES eingereicht haben.

F4. Wie kann ich herausfinden, von welchen E-Mail-Adressen Beschwerden kamen?

Zum Schutz der Identitäten der Empfänger, die sich beschwert haben, können wir die E-Mail-Adressen, die sich über Ihre E-Mail beschwert haben, nicht auflisten.

Anstatt sich auf das Entfernen einzelner Empfänger aus Ihren Listen zu konzentrieren, empfehlen wir, dass Sie das Problem ermitteln, das Anlass zu den Beschwerden gab. Wir empfehlen, dass Sie zunächst Ihre Kundenakquise überprüfen und Kunden, die Ihre E-Mails nicht explizit angefordert haben, aus Ihren Listen entfernen. Sie sollten auch den Inhalt Ihrer E-Mails analysieren, um zu verstehen, warum sich Ihre Empfänger beschweren.

F5. Kann ich eine Beispiel-E-Mail erhalten?

Zum Schutz der Identitäten der Empfänger, die sich beschwert haben, können wir keine Kopien der E-Mails, die Anlass zur Beschwerde gaben, zur Verfügung stellen.

F6. Was soll ich tun, wenn mir in einer Benachrichtigung mitgeteilt wird, dass mein Konto geprüft wird oder dass für mich das Senden aufgrund direkter Beschwerden unterbrochen wird?

Ändern Sie Ihre Sendeabläufe sofort, sodass Sie Nachrichten nur an Empfänger senden, die diese abonniert haben. Stellen Sie außerdem sicher, dass Sie die Art von Inhalten senden, die die Empfänger abonniert haben. Nachdem Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie in Ihrer Nachricht detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt.

Wenn Sie innerhalb von drei Wochen keine Überprüfung anfordern und wir weiterhin Beschwerden direkt von Empfängern erhalten, setzen wir die Möglichkeit, mit Ihrem Konto E-Mails zu versenden ggf. aus.

Häufig gestellte Fragen zu SES-Beschwerden über E-Mail-Anbieter

Dieses Thema enthält Informationen zu Beschwerden, die SES über E-Mail-Anbieter (auch Postfachanbieter genannt) erhält. Allgemeine Informationen, die für alle Arten von Beschwerden gelten, finden Sie unter Beschwerden – Häufig gestellte Fragen.

F1. Wie wird diese Art Beschwerde gemeldet?

Ein E-Mail-Anbieter hat SES gemeldet, dass eine beträchtliche Anzahl seiner Kunden Ihre E-Mails als Spam markiert hat. Der Bericht wurde SES auf andere Weise als über die in der beschriebenen Feedback-Schleifen zur Verfügung gestelltHäufig gestellte Fragen zu SES-Beschwerden über Feedback-Schleifen.

F2. Sind diese Beschwerden in der Statistik der Beschwerdequote enthalten, die in der SES-Konsole angezeigt wird und von der GetSendStatistics API zurückgesendet wird?

Nein. Die Statistik der Beschwerdequote, die Sie über die SES-Konsole oder die `GetSendStatistics` API abrufen, umfasst nur Beschwerden, die SES über Feedback-Loops erhält.

F3. Warum wurde ich nicht durch Feedback-Benachrichtigungen per E-Mail oder über Amazon SNS über diese Beschwerden informiert?

Die Weiterleitung von Feedback per E-Mail und Amazon SNS SNS-Benachrichtigungen umfassen nur Beschwerden, die SES über Feedback-Schleifen erhält.

F4. Wie kann ich herausfinden, von welchen E-Mail-Adressen Beschwerden kamen?

E-Mail-Anbieter legen diese Informationen in der Regel nicht offen. Anstatt sich jedoch auf das Entfernen einzelner Empfänger aus der Liste zu konzentrieren, muss für Sie das Ermitteln und Korrigieren des zugrunde liegenden Problems im Mittelpunkt stehen. Beginnen Sie damit, Ihren Listenakquisitionsprozess und den Inhalt Ihrer E-Mails zu prüfen, um zu verstehen, warum die Empfänger Ihre E-Mails möglicherweise nicht erhalten möchten.

F5. Kann ich eine Beispiel-E-Mail erhalten?

Nein. E-Mail-Anbieter stellen in der Regel keine Beispiel-E-Mail bereit.

F6. Was soll ich tun, wenn mir in einer Benachrichtigung mitgeteilt wird, dass mein Konto geprüft wird oder dass für mich das Versenden aufgrund von Beschwerden durch E-Mail-Anbieter unterbrochen wird?

Identifizieren Sie die Ursache des Problems und korrigieren Sie es. Nachdem Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie in Ihrer Nachricht detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt. Wenn Sie innerhalb von drei Wochen keine Überprüfung anfordern und wir weiterhin Beschwerden von E-Mail-Anbietern erhalten, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos zum Versenden von E-Mails.

Pseudo-E-Mail-Adressen für Spam – Häufig gestellte Fragen

F1. Was sind Pseudo-E-Mail-Adressen für Spam?

Ein Spamtrap ist eine spezielle E-Mail-Adresse, die von einem Internetdienstanbieter (ISP), einem E-Mail-Anbieter oder einer Anti-Spam-Organisation unterhalten wird. Da diese Adresse niemals auf legitime Weise für den Erhalt von E-Mails registriert wird, wissen die Organisationen, die diese Pseudo-E-Mail-Adressen für Spam unterhalten, dass jeder, der E-Mails an diese Adressen sendet, höchstwahrscheinlich fragwürdige E-Mail-Methoden anwendet.

F2. Wie werden Spamtraps eingerichtet?

Spamtrap-Adressen können auf mehrere Weisen eingerichtet werden. Sie können von Adressen konvertiert werden, die einmal gültig waren, aber für einen längeren Zeitraum nicht genutzt wurden

(und als nicht zustellbar zurückgesendet wurden). Sie können auch Adressen sein, die einfach als Spamfallen eingerichtet wurden. Sie können ungewöhnliche Adressen sein, die schwer zu erraten sind, und manchmal sind es Adressen, die echten Adressen ähnlich sind (sie weisen z. B. einen Tippfehler in einem gängigen Domänennamen auf). Häufig, aber nicht immer, gelangen Spamtraps in die Welt, indem sie auf verschiedene Arten und Weisen im Internet platziert werden.

F3. Woher weiß SES, ob ich an Spamtraps sende?

Bestimmte Organisationen, die Spamtraps einsetzen, senden SES-Benachrichtigungen, wenn ihre Spamtraps von SES-Absendern getroffen werden.

F4. Wie verwendet SES die Spamtrap-Berichte?

Wir überprüfen die Berichte. Wenn wir feststellen, dass Ihr Konto E-Mails an Spamfallen sendet, legen wir eine Prüfung für Ihr Konto fest und bitten Sie, das zugrunde liegende Problem zu beheben. Wenn Sie das Problem vor Ablauf des Überprüfungszeitraums nicht beheben, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, weitere E-Mails zu senden. Wenn Ihr Problem mit Spamfallen besonders gravierend ist, können wir die Fähigkeit Ihres Kontos zum Versenden von E-Mails mit sofortiger Wirkung unterbrechen, ohne zuerst eine Prüfung für Ihr Konto festzulegen.

F5. Was soll ich tun, wenn mir in einer Benachrichtigung mitgeteilt wird, dass mein Konto geprüft wird oder dass für mich das Senden aufgrund eines Problems mit Spamfallen unterbrochen wird?

Zuerst sollten Sie das Problem beheben, weswegen wir eine Prüfung für Ihr Konto festgelegt oder Ihre Fähigkeit zum Versenden von E-Mails unterbrochen haben. Melden Sie sich anschließend bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie in Ihrer Nachricht detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt. Wenn wir Ihnen zustimmen, dass die von Ihnen vorgenommenen Änderungen für das Problem angemessen sind, beenden wir den Überprüfungszeitraum und heben die Sendeunterbrechung für Ihr Konto auf.

Aufgrund der Art und Weise, wie Spamfallen-Treffer gemeldet werden, kann es mindestens drei Wochen dauern, bis wir bestimmen können, ob das Problem durch die von Ihnen vorgenommenen Änderungen behoben wird.

F6. Wie viele Treffer für Spamfallen kann ich haben, bevor eine Prüfung für mein Konto festgelegt wird oder die Fähigkeit meines Kontos zum Versenden von E-Mails unterbrochen wird?

Wir legen nicht die genaue Anzahl von Spamfallen-Treffer offen, die uns dazu bewegen, Maßnahmen für Ihr Konto zu ergreifen. Bitte beachten Sie jedoch, dass sogar eine kleine Anzahl von Spamfallen-Treffern Ihrem guten Ruf als Sender bereits schaden kann. Sie sollten Spamfallen-Berichte daher ernst nehmen.

F7. Legen Sie die Adressen der Spamfallen offen?

Nein. Spamfallen sind nur wirksam, wenn solange sie vertraulich bleiben. Spamtrap-Organisationen geben nur preis, dass hier tatsächlich Treffer für Spamtraps vorliegen, nicht die tatsächlichen Spamtrap-Adressen.

F8. Was kann ich tun, um das Senden an Spamfallen zu verhindern?

Gehen Sie folgendermaßen vor, um das Risiko, an Spamfallen zu senden, zu senken:

- Kaufen oder mieten Sie keine E-Mail-Adressen und geben Sie keine E-Mail-Adressen weiter. Verwenden Sie nur E-Mail-Adressen, die Ihre E-Mails explizit angefordert haben.
- Bitten Sie Benutzer, ihre E-Mail-Adressen auf Webformularen zwei Mal anzugeben, und stellen Sie sicher, dass beide Adressen übereinstimmen, bevor das Formular gesendet werden kann.
- Verwenden Sie bei der Registrierung neuer Benutzer ein Double-Opt-in-Verfahren für die doppelte Anmeldung. Das bedeutet Folgendes: Wenn sich neue Benutzer registrieren, senden Sie Ihnen eine Bestätigungs-E-Mail, auf die sie klicken müssen, bevor sie weitere E-Mails erhalten.
- Stellen Sie sicher, dass Sie die Adressen, die permanent unzustellbar sind, aus Ihrer Liste löschen, so dass sie entfernt werden, lange bevor sie zu Spamfallen konvertiert werden.
- Überwachen Sie unbedingt die Interaktion auf Seiten Ihrer Empfänger und senden Sie keine E-Mails mehr an Empfänger, die in letzter Zeit keine Interaktionen mit Ihren E-Mails oder Ihrer Website gezeigt haben. Der richtige Zeitrahmen hierfür hängt von Ihrem Anwendungsfall ab. Im Allgemeinen jedoch, wenn Benutzer mehrere Monate lang Ihre E-Mails nicht geöffnet oder angeklickt haben, sollten Sie in Betracht ziehen, sie zu entfernen, es sei denn, Sie haben Nachweise dafür, dass sie Ihre E-Mails erhalten möchten.
- Seien Sie vorsichtig mit Re-Engagement-Kampagnen, bei denen Sie absichtlich Personen kontaktieren, die in letzter Zeit keine Interaktion mit Ihnen gezeigt haben. Solche Bemühungen

sind meist äußerst riskant und können häufig zu Problemen nicht nur mit dem Versenden an Spamfallen, sondern auch mit Unzustellbarkeit und Beschwerden führen.

- Senden Sie eine Opt-in-Nachricht an Ihre gesamte Mailing-Liste und behalten Sie nur die Empfänger bei, die auf den Verifizierungslink klicken. Diese Prozedur hilft nicht nur beim Entfernen inaktiver Empfänger aus Ihrer Liste, sondern auch beim Entfernen von Spamfallen-Adressen. Die Anwendung dieser Methode wird jedoch nicht empfohlen, wenn Sie vermuten, dass Ihre Mailing-Liste unter Umständen eine Menge ungültiger Adressen enthält oder wenn Ihr Konto bereits ein Problem mit Unzustellbarkeit hat, da sich mit ihr die Unzustellbarkeitsquote Ihres Kontos weiter erhöhen kann.

Manuelle Überprüfung – Häufig gestellte Fragen

F1. Was soll ich tun, wenn mir in einer Benachrichtigung mitgeteilt wird, dass mein Konto geprüft wird oder dass für mich das Versenden aufgrund einer manuellen Überprüfung unterbrochen wird?

Ein SES-Ermittler hat ein erhebliches Problem bei Ihrem Versand festgestellt. Typische Probleme sind unter anderem folgende:

- Ihre Sendevorgänge verstoßen gegen die AWS Acceptable Use Policy (AUP).
- Ihre E-Mails scheinen unerwünscht zu sein.
- Ihre Inhalte beziehen sich auf Phishing (einschließlich simuliertem Phishing).
- Ihr Inhalt ist ansonsten mit einem Anwendungsfall verknüpft, den SES nicht unterstützt.

Wenn wir glauben, dass das Problem behoben werden kann, legen wir über einen bestimmten Zeitraum hinweg eine Prüfung für Ihr Konto fest. Während Ihr Konto geprüft wird, sollten Sie Änderungen an Ihrem E-Mail-Sendeverhalten vornehmen, um das Problem zu beheben.

Wenn wir nicht glauben, dass das Problem behoben werden kann, oder wenn das Problem sehr gravierend ist, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos zum Versenden von E-Mails, ohne zuerst eine Prüfung für Ihr Konto festzulegen.

F2. Welche Probleme könnten dazu führen, dass eine manuelle Überprüfung für mein Versenden von E-Mails durchgeführt wird?

Es gibt verschiedene Probleme, die uns dazu bewegen könnten, mit einer manuellen Überprüfung Ihres Kontos zu beginnen. Hierzu gehören unter anderem folgende Gründe:

- Empfänger wenden sich an SES, um sich über E-Mails zu beschweren, die von Ihrem Konto gesendet wurden.
- Wir erkennen ungewöhnliche Änderungen in Ihren E-Mail-Versandmustern.
- Unsere Spam-Filter finden Merkmale Ihrer E-Mails, die für unerwünschte oder minderwertige Inhalte typisch sind.

Wenn wir für Ihr Konto eine Prüfung festlegen oder die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrechen, senden wir Ihnen eine Benachrichtigung. In den meisten Fällen enthält diese Benachrichtigung Informationen über das Problem und über die nächsten Schritte, die Sie ergreifen können.

F3. Was sind "unerwünschte" E-Mails?

Unerwünschte E-Mails sind E-Mails, die der Empfänger nicht explizit angefordert hat. Hierzu gehören Fälle, bei denen sich ein Empfänger für eine bestimmte Art von E-Mails anmeldet (z. B. Benachrichtigungen) und ihm stattdessen eine andere Art von E-Mails gesendet wird (z. B. Werbung).

Wenn wir für Ihr Konto eine Prüfung festlegen oder die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrechen, senden wir Ihnen eine Benachrichtigung. Wenn Sie eine Benachrichtigung erhalten, dass wir aufgrund eines Problems mit unerwünschten E-Mails eine dieser Maßnahmen ergreifen, melden Sie sich bei der AWS Konsole an und rufen Sie das Support Center auf. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Schließen Sie die folgenden Informationen in Ihre Nachricht ein:

- Sind alle von Ihnen gesendeten Nachrichten vom Empfänger explizit angefordert und entsprechen sie der AWS Acceptable Use Policy?
- Haben Sie die E-Mail-Adressen auf andere Wege erhalten als dadurch, dass ein Kunde explizit mit Ihnen oder Ihrer Website in Interaktion getreten ist und E-Mails angefordert hat? Sie sollten erklären, wie Sie Ihre Mailing-Liste zusammengestellt haben.
- Wie funktionieren Ihre Prozesse zum Abonnieren bzw. Kündigen des Abonnements? Sie sollten Ihre Links für die Anmeldung und die Abmeldung einfügen.

F4. Was soll ich tun, wenn mir in einer Benachrichtigung mitgeteilt wird, dass mein Konto geprüft wird oder dass für mich das Versenden aufgrund einer manuellen Überprüfung unterbrochen wird?

Identifizieren Sie die Ursache des Problems und korrigieren Sie es. Nachdem Sie Änderungen vorgenommen haben, von denen Sie glauben, dass sie das Problem lösen, melden Sie sich bei der AWS Konsole an und gehen Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben. Geben Sie in Ihrer Nachricht detaillierte Informationen über die Schritte an, die Sie zur Lösung des Problems unternommen haben, und wie durch sie verhindert wird, dass das Problem erneut auftritt. Wenn wir Ihnen zustimmen, dass die von Ihnen vorgenommenen Änderungen für das Problem angemessen sind, beenden wir den Überprüfungszeitraum für Ihr Konto.

F5. Welche Arten von Problemen sehen Sie als "korrigierbar" an?

Generell gehen wir davon aus, dass der Fall korrigierbar ist, wenn Sie bisher stets gute Versandmethoden anwendeten und wenn es Schritte gibt, die Sie unternehmen können, um das problematische Senden zu eliminieren, während Sie mit dem Großteil Ihres E-Mail-Versands fortfahren. Wenn Sie beispielsweise drei verschiedene Arten von E-Mails senden und nur eine Art problematisch ist, können Sie unter Umständen einfach den problematischen Sendevorgang stoppen und den Rest Ihres Versands weiterführen.

F6. Was geschieht, wenn ich die Ursache des Problems nicht finden kann?

Sie können sich bei der AWS Konsole anmelden und das Support Center aufrufen. Antworten Sie auf den Fall, den wir in Ihrem Namen geöffnet haben, und fordern Sie ein Beispiel der E-Mail an, die das Problem verursacht hat.

DNS-Blackhole-Liste (DNSBL) FAQs

Auf dem Domainnamensystem basierende Blackhole-Listen (DNSBLs) — manchmal auch als Echtzeit-Blackhole-Listen (RBLs), Ablehnungslisten, Blocklisten oder Blacklisten bezeichnet — sollen E-Mail-Anbieter über IP-Adressen informieren, von denen der Verdacht besteht, dass sie unerwünschte E-Mails versenden.

Verschiedene haben unterschiedliche Auswirkungen auf die Zustellbarkeit von E-Mails. DNSBLs In diesem Thema wird beschrieben, wie DNSBLs sich die Zustellung von E-Mails auswirkt, die Sie mit Amazon SES versenden, sowie unsere Richtlinien zum Entfernen von Amazon SES SES-IP-Adressen DNSBLs.

> **Note**
>
> In diesem Thema geht es um die DNSBLs , die E-Mail-Anbieter verwenden, um eingehende Nachrichten zu blockieren. Weitere Informationen darüber, wie Amazon SES ausgehende E-Mail-Nachrichten blockiert, die an Empfänger gesendet wurden, deren E-Mail-Adressen zuvor Unzustellbarkeitsnachrichten generiert haben, finden Sie unter Globale Unterdrückungsliste in Amazon SES.

F1. Wie DNSBLs wirkt sich das auf die E-Mail-Zustellung aus?

Verschiedene DNSBLs haben unterschiedliche Auswirkungen auf die erfolgreiche Zustellung einer Nachricht. Große E-Mail-Anbieter — darunter Gmail, Hotmail, AOL und Yahoo — scheinen nur eine sehr geringe Anzahl hoch angesehener E-Mail-Anbieter zu erkennen DNSBLs, wie sie beispielsweise von Spamhaus angeboten werden. Unserer Erfahrung nach haben andere in der DNSBLs Regel nur geringe Auswirkungen, obwohl einige E-Mail-Systeme bestimmte gegenüber anderen hervorheben. DNSBLs

Schließlich verfügen viele E-Mail-Anbieter oft über eigene interne Sperrlisten. E-Mail-Anbieter behandeln diese Listen in der Regel streng vertraulich und teilen sie selten mit der Öffentlichkeit. Wenn eine IP-Adresse auf einer dieser Listen steht, kann dies erhebliche Auswirkungen auf Ihre Fähigkeit zum Versenden von E-Mails an Empfänger haben, die diesen Anbieter nutzen.

F2. Wie landen IP-Adressen am Ende DNSBLs?

Es gibt verschiedene Möglichkeiten, die dazu führen, dass eine IP-Adresse auf einer DNSBL landet. IP-Adressen können hinzugefügt werden, DNSBLs wenn E-Mails an einen Spamtrap gesendet werden. Eine Spamfalle ist eine E-Mail-Adresse, die zu keiner echten Person gehört. Die einzige Aufgabe von Spamfallen besteht darin, Spam zu sammeln und Spammer zu identifizieren. Einige ermöglichen es DNSBLs auch einzelnen Benutzern, IP-Adressen einzureichen. Einige erlauben es Benutzern DNSBLs sogar, ganze IP-Adressbereiche einzureichen. Andere DNSBLs werden durch Beiträge von E-Mail-Administratoren verwaltet und können IP-Adressen enthalten, von denen Administratoren glauben, dass sie ihre eigenen Systeme missbrauchen.

F3. Wie verhindert Amazon SES, dass seine IP-Adressen angezeigt werden DNSBLs?

Unsere Systeme suchen nach Anzeichen eines Missbrauchs. Wenn wir Sendemuster oder andere Merkmale erkennen, die dazu führen, dass eine IP-Adresse auf die DNSBL gesetzt wird, senden wir eine Benachrichtigung an den Sender. Wenn die Situation schwerwiegend ist oder wenn der Sender das Problem nicht behebt, nachdem wir ihn benachrichtigt haben, unterbrechen wir die Fähigkeit des Senders zum Versenden von E-Mails, bis er das Problem gelöst hat. Die Durchsetzung unserer Senderichtlinien auf diese Weise trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass unsere IP-Adressen landen DNSBLs.

F4. Kann Amazon SES seine IP-Adressen aus einer DNSBL entfernen lassen?

Bei SES shared beobachten wir aktiv IPs, ob sich DNSBLs dies auf die Zustellung im gesamten Amazon SES SES-Service oder auf die Fähigkeit auswirken könnte, E-Mails an Empfänger zu senden, die große E-Mail-Anbieter wie Gmail, Yahoo, AOL und Hotmail verwenden. Die von Spamhaus DNSBLs angebotenen Produkte fallen in diese Kategorie. Wenn eine unserer IP-Adressen in einer Liste erscheint, die eine dieser Kriterien erfüllt, ergreifen wir sofort Maßnahmen, um diese Adresse so schnell wie möglich von der DNSBL zu entfernen.

Wir beobachten nicht DNSBLs , dass sie sich wahrscheinlich nicht auf die Zustellung im gesamten Amazon SES SES-Service auswirken oder die keine messbaren Auswirkungen auf die Zustellung an wichtige E-Mail-Anbieter haben. Die von SORBS und UCEPROTECT DNSBLs angebotenen Produkte fallen in diese Kategorie. Aufgrund der spezifischen Auflistungs- und Löschverfahren der Anbieter, die diese Listen betreiben, können wir unsere IP-Adressen nicht aus diesen Listen entfernen lassen.

Für dedizierte IP-Adressen (verwaltet oder Standard), die in einer RBL von E-Mail-Empfängern aufgeführt sind, liegt es nicht in der Verantwortung von SES, diese aus der Liste zu streichen, IPs und Sie müssen die Entfernung direkt beim RBL-Administrator beantragen.

F5. Ein E-Mail-Anbieter meine E-Mail ablehnt, weil die sendende IP-Adresse von einem anderen DNSBL als Spamhaus aufgeführt wird. Was sollte ich tun?

Bestätigen Sie zunächst, dass die Nachricht aufgrund einer DNSBL wirklich blockiert wurde. Wenn Ihre E-Mail abgelehnt wurde, weil die sendende IP-Adresse einer DNSBL hinzugefügt wurde, erhalten Sie eine Unzustellbarkeitsbenachrichtigung, in der der DNSBL-Anbieter namentlich erwähnt wird, wie im folgenden Beispiel gezeigt:

```
554 5.7.1 Service unavailable; Client host [192.0.2.0] blocked using DNSBLName;
 See: http://www.example.com/query/ip/192.0.2.0
```

Wenn Sie eine Unzustellbarkeitsbenachrichtigung erhalten haben, diese jedoch keine Informationen wie die im vorigen Beispiel gezeigte Nachricht enthält, dann hat der E-Mail-Anbieter Ihre Nachricht höchstwahrscheinlich aus einem Grund abgelehnt, der nichts mit einer DNSBL zu tun hat.

Wenn Sie bestätigen können, dass ein E-Mail-Anbieter Ihre E-Mail blockiert, da sich die sendende IP-Adresse auf einer DNSBL befindet, gibt es einige Maßnahmen, die Sie ergreifen können:

- Wenden Sie sich an den Postmaster der Domäne, die Ihre Nachricht abgelehnt hat, und bitten Sie um eine Ausnahmeregelung von ihrer Spam-Filterrichtlinie. Einige Postmaster bieten Support-Prozesse, die möglicherweise auf einer Postmaster-Seite veröffentlicht und beschrieben werden. Wenn die Domain, die Sie kontaktieren möchten, ihre Postmaster-Supportrichtlinien nicht veröffentlicht, können Sie den Postmaster möglicherweise kontaktieren, indem Sie eine E-Mail an postmaster@ senden*example.com*, wo sich die fragliche Domain befindet. *example.com* Gemäß RFC 5321 müssen Domänen über ein Postmaster-Postfach verfügen.

  Wenn Sie sich an den Postmaster wenden, geben Sie die Unzustellbarkeitscodes an, die Sie empfangen haben, die Headers der E-Mail, die Sie zu senden versuchen, eine Einschätzung der Auswirkungen der DNSBL auf Ihre E-Mail-Zustellung und Informationen darüber, warum Ihre E-Mail Ihrer Meinung nach fälschlicherweise blockiert wird. Je mehr Informationen Sie angeben können, um dem Postmaster aufzuzeigen, das Sie legitime E-Mails senden, desto größer ist die Wahrscheinlichkeit, dass der Postmaster für Sie eine Ausnahme machen wird.
- Wenn der E-Mail-Anbieter nicht reagiert oder nicht bereit ist, seine Richtlinien zu ändern, sollten Sie eine dedizierte IP-Adresse verwenden. Dedizierte IP-Adressen sind IP-Adressen, die nur von Ihnen verwendet werden können. Durch die Umsetzung eines guten Sendeverhaltens, können Sie dafür sorgen, dass Ihre Quoten für Nutzerbindung hoch und für unzustellbare Nachrichten, Beschwerden

und Spamfallen-Treffer niedrig bleiben. Gute Versandpraktiken können dazu beitragen, dass Ihre Adressen nicht landen. DNSBLs

F6. E-Mails, die ich an Gmail, Yahoo, Hotmail oder einen anderen wichtigen Anbieter sende, werden an den Spam-Ordner gesendet. Geschieht dies, weil sich meine sendende IP-Adresse auf einer DNSBL befindet?

Wahrscheinlich nicht. Wenn eine IP-Adresse von einer DNSBL mit erheblichen Auswirkungen aufgeführt wird, wie z. B. einer DNSBLs von Spamhaus, lehnen große E-Mail-Anbieter E-Mails von dieser IP-Adresse vollständig ab, anstatt sie in den Spam-Ordner zu senden.

Wenn große E-Mail-Anbieter E-Mail-Nachrichten annehmen (anstatt sie abzulehnen), ziehen sie gewöhnlich das Benutzerengagement in Betracht, wenn sie bestimmen, ob die Nachricht im Posteingang oder im Spam-Ordner zu platzieren ist. Nutzer-Engagement bezieht sich auf die Art und Weise, wie Benutzer mit den Nachrichten interagiert haben, die Sie zuvor gesendet haben.

Um die Chancen zu erhöhen, dass Ihre Nachrichten auch im Postfach Ihrer Kunden ankommen, sollten Sie alle der folgenden bewährten Methoden implementieren:

- Mieten oder kaufen Sie niemals Listen mit E-Mail-Adressen. Die Anmietung oder der Kauf von Listen ist ein Verstoß gegen die AWS Richtlinie zur akzeptablen Nutzung (AUP) und auf der Amazon SES-Plattform unter keinen Umständen zulässig.
- Senden Sie E-Mails nur an Kunden, die E-Mails von Ihnen explizit angefordert haben. In vielen Ländern und Jurisdiktionen auf der ganzen Welt ist es illegal, E-Mail-Nachrichten an Empfänger zu senden, die nicht ausdrücklich mit dem Empfang von E-Mail-Nachrichten von Ihnen einverstanden sind.
- Stoppen Sie das Senden von E-Mails an Kunden, die Nachrichten, die Sie in den letzten 30 bis 90 Tage gesendet haben, nicht geöffnet oder auf Links in diesen geklickt haben. Dieser Schritt kann dazu beitragen, Ihre Interaktionsraten hoch zu halten, was die Wahrscheinlichkeit erhöht, dass die Nachrichten, die Sie in Zukunft senden, in den Posteingängen der Empfänger eintreffen.
- Verwenden Sie konsistente Designelemente und Schreibstile in jeder gesendeten Nachricht, um sicherzustellen, dass Kunden Nachrichten von Ihnen leicht erkennen können.
- Verwenden Sie E-Mail-Authentifizierungsmechanismen, wie z. B. SPF und DKIM.
- Wenn Kunden ein Web-Formular verwenden, um Ihre Inhalte zu abonnieren, senden Sie Ihnen eine E-Mail, um zu bestätigen, dass sie von Ihnen E-Mails erhalten möchten. Senden Sie ihnen

keine zusätzlichen E-Mails, bis sie bestätigen, dass sie von Ihnen E-Mails erhalten möchten. Dieser Prozess wird als bestätigte Abonnements oder Double-Opt-In bezeichnet.

- Machen Sie es Ihren Kunden leicht, sich abzumelden und berücksichtigen Sie Abmeldeanforderungen sofort.
- Wenn Sie E-Mails senden, die Links enthalten, überprüfen Sie diese Links anhand der Spamhaus Domain Block List (DBL). Wenn Sie Ihre Links testen möchten, verwenden Sie das Domain Lookup-Tool auf der Spamhaus-Website.

Durch die Implementierung dieser Methoden können Sie Ihre Zuverlässigkeit als Sender verbessern, wodurch sich die Wahrscheinlichkeit erhöht, dass die von Ihnen gesendeten E-Mails den Posteingang der Empfänger erreichen. Die Implementierung dieser Praktiken kann Sie auch dabei unterstützen, die Unzustellbarkeits- und Beschwerdequoten für Ihr Konto niedrig zu halten, und verringern das Risiko, dass E-Mails an Spamfallen gesendet werden.

Amazon SES SES-Metriken zum Senden von E-Mails FAQs

Amazon SES sammelt verschiedene Metriken über die E-Mails, die Sie senden. Mit diesen Metriken können Sie die Effektivität Ihres E-Mail-Programms analysieren und wichtige Statistiken überwachen, wie zum Beispiel Ihre Unzustellbarkeits- und Beschwerdequoten.

Dieser Abschnitt enthält FAQs die folgenden Themen im Zusammenhang mit Kennzahlen zum Senden von E-Mails:

- Allgemeine Fragen
- Öffnungsnachverfolgung
- Klicknachverfolgung

> **Note**
>
> Die Ereignisverfolgung hängt vom E-Mail-Dienstanbieter (ESP) des Empfängers ab und davon, wie er seine Datenschutzeinstellungen konfiguriert hat, die außerhalb der Kontrolle von Amazon SES liegen. Die Anzahl der Tracking-Ereignisse kann unter folgenden Bedingungen verzerrt werden (ungenaue Zählungen zurückgeben):
>
> - Der E-Mail-Empfänger verwendet einen E-Mail-Dienstanbieter (ESP), der seine Privatsphäre schützt.

- Der E-Mail-Empfänger erteilt seinem ESP ausdrücklich keine Erlaubnis, seine Daten weiterzugeben.
- Der ESP des E-Mail-Empfängers speichert Bilder oder Links im Cache, SES kann nur das erste Öffnen zählen, kann aber nachfolgende Öffnungen nicht zählen.

Allgemeine Fragen

F1. Wie lange sammelt Amazon SES weiter Öffnungs- und Klickmetriken, nachdem eine E-Mail zugestellt wurde?

Amazon SES sammelt Öffnungs- und Klickmetriken 60 Tage lang, nachdem die jeweilige E-Mail gesendet wurde.

F2. Wenn ein Benutzer eine E-Mail mehrmals öffnet oder auf mehrfach auf einen Link in einer E-Mail klickt, wird dann jedes dieser Ereignisse separat nachverfolgt?

Wenn ein Empfänger eine E-Mail mehrmals öffnet, zählt Amazon SES jede Öffnung als einmaliges Öffnungsereignis. Ebenso gilt: Wenn ein Empfänger mehrfach auf denselben Link klickt, zählt Amazon SES jeden Klick als einmaliges Klickereignis. Diese Zählungen können jedoch durch die oben im Notizfeld beschriebenen Szenarien verzerrt werden.

F3. Sind Öffnungs- und Klickmetriken aggregiert oder können sie bis auf Empfängerebene gemessen werden?

Öffnungen und Klicks werden auf Empfängerebene nachverfolgt. Mithilfe der Nachverfolgung von Öffnungs- und Klickereignissen können Sie bestimmen, welche Empfänger eine E-Mail geöffnet oder auf einen Link in einer E-Mail geklickt haben.

F4. Kann ich Öffnungs- und Klickmetriken mit der Amazon-SES-API abrufen?

Die Amazon-SES-API bietet keine Methode zum Abrufen von Öffnungs- und Klickmetriken. Sie können jedoch die Öffnungs- und Klickmetriken für Amazon SES mithilfe der CloudWatch API abrufen. Sie können beispielsweise die verwenden, AWS CLI um Klickmetriken mithilfe der CloudWatch API abzurufen, indem Sie den folgenden Befehl ausführen:

```
aws cloudwatch get-metric-statistics --namespace AWS/SES --metric-name Click \
```

```
  --statistics Sum --period 86400 --start-time 2017-01-01T00:00:00Z \
  --end-time 2017-12-31T23:59:59Z
```

Der oben gezeigte Befehl ruft die Gesamtanzahl an Klickereignissen für jeden Tag im Jahr 2017 ab. Zum Abrufen von Öffnungsmetriken ändern Sie den Wert des `metric-name`-Parameters in `Open`. Sie können auch die Parameter `start-time` und `end-time` so bearbeiten, dass der Analysezeitraum geändert wird, oder den `period`-Parameter für eine genauere Analyse ändern.

Öffnungsnachverfolgung

F1. Wie funktioniert die Öffnungsnachverfolgung?

In jede E-Mail, die über Amazon SES gesendet wird, wird ein transparentes GIF-Bild mit einer Breite und Höhe von jeweils 1 Pixel eingefügt, das einen eindeutigen Verweis auf diese Bilddatei enthält. Wenn das Bild heruntergeladen wird, kann SES genau feststellen, welche Nachricht von wem geöffnet wurde.

Standardmäßig wird dieses Pixel am Ende der E-Mail eingefügt. Die Anwendungen einiger E-Mail-Anbieter beschneiden jedoch die Vorschau einer E-Mail, wenn sie eine bestimmte Größe überschreitet, und stellen möglicherweise einen Link zur Anzeige der restlichen Nachricht zur Verfügung. In diesem Szenario wird das SES-Pixelbild zur Nachverfolgung nicht geladen und verfälscht die Öffnungsraten, die Sie nachverfolgen möchten. Um dies zu umgehen, können Sie das Pixel optional an den Anfang der E-Mail oder an eine andere Stelle setzen, indem Sie den Platzhalter `{{ses:openTracker}}` in den E-Mail-Text einfügen. Sobald SES die Nachricht mit dem Platzhalter empfängt, wird sie durch ein Pixelbild zur Nachverfolgung von Öffnungen ersetzt.

> **Important**
>
> Fügen Sie einfach einen `{{ses:openTracker}}`-Platzhalter hinzu, da mehr als einer dazu führt, dass ein `400 BadRequestException`-Fehlercode zurückgegeben wird.

Durch das Hinzufügen dieses Trackingpixels wird die Darstellung der E-Mail nicht verändert.

F2. Ist die Öffnungsnachverfolgung standardmäßig aktiviert?

Die Öffnungsnachverfolgung ist standardmäßig für alle Amazon-SES-Benutzer verfügbar. Zur Verwendung der Öffnungsnachverfolgung führen Sie folgende Aufgaben aus:

1. Erstellen Sie einen Konfigurationssatz.
2. Erstellen Sie im Konfigurationssatz ein Ereignisziel.
3. Konfigurieren Sie das Ereignisziel so, dass Benachrichtigungen zu Öffnungsereignissen an einem Ziel veröffentlicht werden.
4. In jeder E-Mail, für die Sie Öffnungen nachverfolgen möchten, geben Sie den Konfigurationssatz an, den Sie in Schritt 1 erstellt haben.

Nähere Informationen zum Aktivieren der Nachverfolgung von Öffnungen über das Ereignisziel eines Konfigurationssatzes finden Sie unter the section called “Ereignisziele erstellen”. Sie können den Pixel-Platzhalter in SMTP-E-Mail verwenden, z. B. in formatierten und unformatierten E-Mails oder E-Mail-Vorlagen.

Weitere Informationen finden Sie unter Überwachen des E-Mail-Versands mithilfe der Ereignisveröffentlichung.

F3. Kann ich das Öffnungs-Trackingpixel bei bestimmten E-Mails auslassen?

Es gibt zwei Möglichkeiten, um das Öffnungs-Trackingpixel bei Ihren E-Mails auszulassen. Bei der ersten Methode wird die E-Mail gesendet, ohne einen Konfigurationssatz anzugeben. Alternativ können Sie einen Konfigurationssatz angeben, der nicht für das Veröffentlichen von Daten zu Öffnungsereignissen konfiguriert ist.

F4. Verfolgen Sie Öffnungen für Klartext-E-Mails?

Die Nachverfolgung von Öffnungen funktioniert nur mit HTML-E-Mails. Da sich die Verfolgung von Öffnungen auf die Aufnahme eines Bildes stützt, ist es nicht möglich, Öffnungsmetriken für Benutzer zu erfassen, die E-Mails mit einem Nur-Text-E-Mail-Client (nicht HTML) öffnen.

Klicknachverfolgung

F1. Wie funktioniert die Klicknachverfolgung?

Zum Nachverfolgen von Klicks ändert Amazon SES jeden Link im Text der E-Mail. Wenn Empfänger einen Link öffnen, werden sie an einen Amazon-SES-Server gesendet und sofort an die Zieladresse weitergeleitet. Wie bei der Öffnungsnachverfolgung ist jeder Umleitungs-Link eindeutig. Auf diese Weise kann Amazon SES bestimmen, welcher Empfänger auf den Link geklickt hat und wann er darauf geklickt hat. Zudem kann die E-Mail, von der aus er auf den Link gelangt ist, bestimmt werden.

> **Important**
>
> Wenn Sie eine einzelne Nachricht an mehrere Empfänger senden, speichert jeder Empfänger denselben Klicknachverfolgungs-Link. Um die Klickaktivität einzelner Empfänger nachzuverfolgen, senden Sie eine E-Mail an einen Empfänger pro Sendevorgang.

F2. Kann ich die Klicknachverfolgung deaktivieren?

Sie können die Klicknachverfolgung deaktivieren, indem Sie den Anker-Tags im HTML-Text Ihrer E-Mail das Attribut `ses:no-track` hinzufügen. Wenn Sie beispielsweise auf die AWS Startseite verlinken, sieht ein normaler Ankerlink wie folgt aus:

```
<a href="https://aws.amazon.com">Amazon Web Services</a>
```

Um die Klicknachverfolgung für diesen Link zu deaktivieren, ändern Sie ihn folgendermaßen:

```
<a ses:no-track href="aws.amazon.com">Amazon Web Services</a>
```

Da `ses:no-track` kein Standard-HTML-Attribut ist, entfernt Amazon SES es automatisch aus der Version der E-Mail, die im Posteingang Ihrer Empfänger eingeht.

Sie können auch die Klicknachverfolgung für alle Nachrichten deaktivieren, die Sie mit einem bestimmten Konfigurationssatz senden. Um die Klicknachverfolgung zu deaktivieren, ändern Sie das Konfigurationssatz-Ereignisziel, sodass keine Klickereignisse erfasst werden.

Nähere Informationen zum Aktivieren und Deaktivieren der Klicknachverfolgung über das Ereignisziel eines Konfigurationssatzes finden Sie unter the section called “Ereignisziele erstellen”.

Weitere Informationen finden Sie unter Überwachen des E-Mail-Versands mithilfe der Ereignisveröffentlichung.

F3. Wie viele Links können in jeder E-Mail verfolgt werden?

Über das Click-Tracking-System können maximal 250 Links verfolgt werden.

F4. Werden Klickmetriken für Links in Klartext-E-Mails erfasst?

Es ist nur möglich, Klicks in HTML-E-Mails zu verfolgen.

F5. Kann ich Links mit eindeutigen Bezeichnern markieren?

Sie können eine unbegrenzte Anzahl von Tags als Schlüssel-Wert-Paare zu Links in Ihrer E-Mail hinzufügen, indem Sie das `ses:tags`-Attribut verwenden. Wenn Sie dieses Attribut verwenden, geben Sie die Schlüssel und Werte mit demselben Format an, das Sie verwenden würden, um Inline-CSS-Eigenschaften zu übergeben: Geben Sie den Schlüssel gefolgt von einem Doppelpunkt (:) und dem Wert ein. Wenn Sie mehrere Schlüssel-Wert-Paare übergeben müssen, trennen Sie die einzelnen Paare durch ein Semikolon (;).

Angenommen, Sie möchten die Tags `product:book, genre:fiction, subgenre:scifi, type:newrelease` zu einem Link hinzufügen. Die resultierende Link sieht in etwa wie folgt aus:

```
<a ses:tags="product:book;genre:fiction;subgenre:scifi;type:newrelease;"
    href="http://www.amazon.com/…/">New Releases in Science Fiction</a>
```

Diese Tags werden an Ihr Ereignisveröffentlichungsziel weitergeleitet, sodass Sie zusätzliche Analysen zu den spezifischen Links durchführen können, auf die Ihre Benutzer geklickt haben.

> **Note**
>
> Link-Tags können die Zahlen 0-9, die Buchstaben A-Z (Groß- und Kleinbuchstaben), Bindestriche (-) und Unterstriche (_) enthalten.

F6. Verwenden nachverfolgte Links das HTTP- oder HTTPS-Protokoll?

Nachverfolgungs-Links verwenden dasselbe Protokoll wie die ursprünglichen Links in Ihrer E-Mail.

Wenn Ihre E-Mail beispielsweise einen Link zu `https://www.amazon.com` enthält, wird der Link durch den Tracking-Link ersetzt, der das HTTPS-Protokoll verwendet. Wenn Ihre E-Mail einen Link zu `http://www.example.com` enthält, wird der Link durch den Tracking-Link ersetzt, der das HTTP-Protokoll verwendet. Wenn Ihre E-Mail beide zuvor erwähnten Links enthält, wird der HTTPS-Link durch einen Nachverfolgungs-Link ersetzt, der das HTTPS-Protokoll verwendet, und der HTTP-Link wird durch einen Nachverfolgungs-Link ersetzt, der das HTTP-Protokoll verwendet.

F7. Ein Link in meiner E-Mail wird nicht nachverfolgt. Warum nicht?

Amazon SES erwartet, dass die Links in Ihren E-Mails korrekt codiert sind URLs. URLs Insbesondere müssen Ihre Links RFC 3986 entsprechen. Wenn ein Link in einer E-Mail nicht ordnungsgemäß

kodiert ist, sehen Empfänger den Link in der E-Mail, aber Amazon SES verfolgt keine Klickereignisse für diesen Link.

Probleme im Zusammenhang mit einer falschen Kodierung treten normalerweise bei solchen Dateien auf URLs , die Abfragezeichenfolgen enthalten. Dies ist beispielsweise der Fall, wenn die URL eines Links in Ihrer E-Mail ein nicht codiertes Leerzeichen in der Abfragezeichenfolge enthält (z. B. das Leerzeichen zwischen "John" und "Doe" im folgenden Beispiel: http://www.example. com/path/to/page? name=John Doe), Amazon SES verfolgt diesen Link nicht. Wenn die URL jedoch stattdessen ein codiertes Leerzeichen verwendet (wie „%20" im folgenden Beispiel: http://www.example. com/path/to/page? name=John%20Doe), Amazon SES verfolgt es wie erwartet.

Schnellsuchindex

Der folgende Index wurde erstellt, um Ihnen zu helfen, Dinge in Amazon SES mithilfe von zwei Arten der Suche schnell zu finden – entweder anhand von Anleitungen oder Konzepten. Die Anleitungen beschreiben bestimmte Vorgehensweisen, während Konzepte umfassendere Erläuterungen bieten.

Teilen Sie uns mit, was Sie denken

Bitte benutzen Sie die Schaltfläche Feedback in der oberen rechten Ecke aus, um uns darüber zu informieren...

- War dieser Index hilfreich?
- Gibt es Anleitungen oder Konzepte, die diesem Index hinzugefügt werden sollten?
- Gab es etwas, von dem Sie meinen, dass es anders hätte kategorisiert werden sollen?

Links zu SES-Anleitungen und -Konzepten

How-tos

SES-Anleitungslinks sind alphabetisch aufgelistet und führen Sie zum entsprechenden Abschnitt, in dem Sie erfahren, wie Sie die von Ihnen ausgewählte Aktion ausführen.

- Weitere Informationen erhalten Sie unter:
  - Im Rahmen der Einrichtung einer benutzerdefinierten MAIL-FROM-Domain einen SPF-Datensatz hinzufügen
  - IP-Pols zuweisen
  - Blockieren Sie SPAM für den E-Mail-Empfang
  - Benutzerdefinierte open/click Domains konfigurieren
  - Konfigurieren von SNS-Benachrichtigungen
  - Herstellen einer Verbindung mit einem SMTP-Endpunkt
  - Erstellen eines Konfigurationssatzes
  - Erstellen einer Domänen-Identität
  - Erstellen einer E-Mail-Adressidentität
  - Ereignisziele erstellen

- Erstellen von IP-Adressenfilter
- Erstellen Sie einen verwalteten IP-Pool, um einen dedizierten IPs (verwalteten) IP-Pool zu aktivieren
- Erstellen von Empfangsregeln
- Erstellen Sie Reputationsalarme mit CloudWatch
- Erstellen einer Sendeautorisierungsrichtlinie mithilfe einer benutzerdefinierten Richtlinie
- Erstellen einer Sendeautorisisierungsrichtlinie mithilfe des Richtliniengenerators
- Erstellen von dedizierten Standard-IP-Pools für dedizierte IP-Adressen (Standard)
- Löschen einer Identität
- Löschen personenbezogener Daten
- Bearbeiten einer Identität
- Aktivieren der E-Mail-Feedback-Weiterleitung
- Exportieren von Zuverlässigkeitsmetriken
- Verlassen der Sandbox
- Erste Schritte mit SES
- Erste Schritte mit dem virtuellen Zustellbarkeitsmanager
- Erteilen von Berechtigungen für den E-Mail-Empfang
- Erhöhen des Durchsatzes
- Erhöhen Ihrer Sendekontingente
- Integrieren in Ihren vorhandenen E-Mail-Server
- Protokollieren von API-Anrufen
- Verwalten von Konfigurationssätzen
- Verwalten von Easy DKIM und BYODKIM
- Überwachen von Versand- und Reputationsmetriken
- Überwachen der Sende-Statistiken
- Überwachen der Nutzungsstatistiken
- Überwachen Ihrer Sende-Quote
- Abrufen von DKIM-Datensätzen für eine Identität
- Abrufen Ihrer SMTP-Anmeldeinformationen
- Überschreibung von Unterdrückung auf Kontoebene mit Unterdrückung auf Konfigurationssatzebene

- Überschreiben der geerbten DKIM-Signatur für eine E-Mail-Adressenidentität
- Unterbrechen der E-Mail-Übertragung
- Veröffentlichen eines MX-Datensatzes
- Missbrauch von AWS Ressourcen melden
- Beantragung dedizierter IP-Adressen
- Anfordern von technischem Support
- Mit dem Berater des virtuellen Zustellbarkeitsmanagers Probleme bei der Zustellbarkeit und der Reputation lösen
- Rufen Sie Ereignisdaten ab von CloudWatch
- Abrufen von Ereignisdaten aus Kinesis Data Firehose
- Abrufen von Ereignisdaten aus SNS
- Senden Sie eine E-Mail mit einem AWS SDK
- Programmgesteuerter Versand von E-Mails
- Senden von E-Mails mit der SES-API
- Senden von E-Mails über SMTP
- Senden von Raw-E-Mails mit einem Anhang über die CLI oder die SES-API
- Senden von Test-E-Mails mit dem Postfachsimulator
- Einrichten von BYODKIM (Verwendung Ihrer eigenen DKIM)
- Einrichten einer DMARC-Richtlinie
- Einrichten von Easy DKIM
- Einrichten des E-Mail-Empfangs
- Einrichten der Ereignisveröffentlichung
- Einrichten einer MAIL FROM-Domäne
- Einrichten der Sendeautorisierung (Aufgaben des Identitätseigentümers)
- Einrichten der Sendeautorisierung (Delegieren der Senderaufgaben)
- Festlegen eines Konfigurationssatzes für das Senden von E-Mail
- Testen Ihrer Verbindung mit der SMTP-Schnittstelle
- Unzustellbarkeits- und Beschwerdequoten
- Verstehen geerbter DKIM-Signatureigenschaften
- Verwenden von Zuverlässigkeitsmetriken

- Verwenden von Softwarepaketen zum Senden von E-Mails
- Verwenden der Abonnementverwaltung
- Verwenden von Vorlagen zum Senden von E-Mails
- Verwenden Ihrer Unterdrückungsliste auf Kontoebene
- Verifizieren einer Domänenidentität
- Verifizieren der Identität einer E-Mail-Adresse
- Anzeigen einer Identität
- Mit dem Dashboard des virtuellen Zustellbarkeitsmanagers die wichtigsten und detaillierten Metriken zur Zustellbarkeit Ihres Kontos anzeigen
- Sehen Sie sich die SNDS-Metriken für spezielle Zwecke an IPs
- Aufwärmen dedizierter IP-Adressen

Concepts

SES-Konzeptlinks sind alphabetisch aufgelistet und führen Sie zu den entsprechenden Kapiteln und Abschnitten, in denen das von Ihnen ausgewählte Konzept erklärt wird.

- Hier finden Sie Informationen zu...
  - Missbrauch von AWS Ressourcen, Bericht
  - Konto-Dashboard
  - Unterdrückungsliste auf Kontoebene
  - Aktionsoptionen für den E-Mail-Empfang
  - „Add Header“-Aktion
  - Nicht-unterstützte Anhangtypen
  - Rücksprungantwort Aktion, zurückgeben
  - BYODKIM (Bring Your Own DKIM – Verwendung Ihrer eigenen DKIM)
  - BYOIP (Bring Your Own IP – Eigene IP mitbringen)
  - Codebeispiele
  - Compliance-Validierung
  - Verwenden der Unterdrückung auf Konfigurationssatzebene
  - Konfigurationssätze
  - Inhaltskodierungen

- Kontoübergreifender Legacy-Benachrichtigungssupport
- Benutzerdefinierte MAIL FROM-Domäne
- Datenschutz
- Dedizierte IP-Adressen
- Dedizierte IP-Adressen (verwaltet)
- Dedizierte IP-Adressen (Standard)
- Authentifizierung Ihrer E-Mails mit DKIM
- DMARC (Domain-based Message Authentication, Reporting and Conformance)
- Einhaltung von DMARC über DKIM
- Einhaltung von DMARC über SPF
- Easy DKIM
- E-Mail-Feedback-Weiterleitungsziel
- Authentifizierung für den E-Mail-Empfang
- Konzepte für den E-Mail-Empfang
- Exemplarische Vorgehensweisen für die E-Mail-Empfangskonsole
- E-Mail-Empfang – Scannen von Malware
- Berechtigungen für den E-Mail-Empfang
- E-Mail-Empfang – Anwendungsfälle
- Einschränkungen für den E-Mail-Empfang
- Authentifizierungsmethoden für den E-Mail-Versand
- Endpunkte
- Ereignis-Benachrichtigungen
- Ereignis-Benachrichtigungen per E-Mail
- Ereignis-Benachrichtigungen über SNS
- Event publishing (Ereignisveröffentlichung)
- FAQs (Häufig gestellte Fragen)
- Globale Unterdrückungsliste
- Unterstützte Header-Felder
- Verwalten der Identitäten
- Verwalten von Identitäten und Zugriff

- Sicherheit der Infrastruktur
- Mit Amazon WorkMail Action integrieren
- IP-basierte Steuerung mit IP-Adressfiltern
- Aufrufen einer Lambda-Funktion
- Listenverwaltung
- Listen und Abonnements
- Protokollierung und Überwachung
- Malware-Erkennung
- Manuelle DKIM-Signierung
- Überwachen des E-Mail-Versands mithilfe der Ereignisveröffentlichung
- Überwachen Ihrer Absenderzuverlässigkeit
- Überwachen der Sender-Aktivität
- Kontingente
- Empfangsregelsatz
- Empfängerbasierte Steuerung mit Empfangsregeln
- Regionen
- Zuverlässigkeitsmetriken
- Zuverlässigkeitsmetriken – Nachrichten
- Ausfallsicherheit
- Aktion „An S3-Bucket liefern“
- Sandbox verlassen
- Sicherheit
- Unterstützte Sicherheitsprotokolle
- Sendeautorisierung
- Sendeautorisierungsrichtlinienanatomie
- Beispiele von Sendeautorisierungsrichtlinien
- Sendeautorisierungsverfahren
- SNDS-Metriken für spezielle IPs
- SNS-Benachrichtigungsinhalte
- SNS-Benachrichtigungsbeispiele

- Veröffentlichung an die SNS-Themen-Aktion
- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)
- Aktion „Regelsatz beenden“
- Abonnementverwaltung
- Support, Anfordern von technischem
- Vorlagen für die benutzerdefinierte E-Mail-Überprüfung
- Fehlersuche
- Verifizierte Identitäten
- Virtueller Zustellbarkeitsmanager
- VPC-Endpunkte

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.