
Amazon Simple Email Service

Entwicklerhandbuch



Amazon Simple Email Service: Entwicklerhandbuch

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, Kunden irrezuführen oder Amazon in irgendeiner Weise herabzusetzen oder zu diskreditieren. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist Amazon SES?	1
Amazon SES	1
Warum Amazon SES verwenden?	1
Amazon SES und andere AWS -Services	1
In diesem Handbuch	2
Quick Start	4
Schritt 1: Registrieren bei AWS	4
Schritt 2: Verifizieren Ihrer E-Mail-Adresse	4
Schritt 3: Senden der ersten E-Mail	4
Schritt 4: Überlegen Sie, wie Sie unzustellbare E-Mails und Beschwerden festlegen	4
Schritt 5: Verlassen der Amazon SES -Sandbox	5
Nächste Schritte	5
Versand von E-Mails	6
Wie sende ich E-Mails mithilfe von Amazon SES?	6
Wie beginne ich?	7
Konzepte	8
Amazon SES und Lieferbarkeit	8
Prozess für den E-Mail-Versand	13
E-Mail-Format und Amazon SES	16
Anmeldeinformationen	18
Erste Schritte	21
Verwenden der Amazon SES Konsole	21
Verwenden von SMTP (Simple Mail Transfer Protocol)	21
Verwenden eines AWS SDK	21
Bevor Sie beginnen	21
Senden einer E-Mail mit der Konsole	22
Senden einer E-Mail mit SMTP	23
Senden einer E-Mail mit einem AWS SDK	34
Migration von einer anderen Lösung zu Amazon SES	49
Einrichten von E-Mail	50
Registrieren bei AWS	51
Verifizieren von Identitäten	52
Abrufen von AWS-Zugriffsschlüsseln	71
Herunterladen eines AWS SDKs	72
Einrichten einer benutzerdefinierten MAIL FROM-Domäne	72
Einrichten von SPF-Datensätzen	78
Einrichten Ihrer SMTP-Anmeldeinformationen	79
Verlassen der -Sandbox	79
Konfigurieren von benutzerdefinierten Öffnungs- und Klickdomänen	85
Einrichten von VPC-Endpunkten	89
E-Mail-Versandmethoden	93
Verwenden der SMTP-Schnittstelle	94
Verwenden der -API	120
Senden einer personalisierten E-Mail	129
E-Mail-Authentifizierungsmethoden	140
Authentifizierung Ihrer E-Mails mit SPF	141
Authentifizierung Ihrer E-Mails mit DKIM	142
Einhaltung von DMARC	154
Verwalten von Sendekontingenten	156
Überwachen Ihrer Sendekontingente	158
Erhöhen Ihrer Sendekontingente	159
Sendekontingente	161
Verwenden der Sendeautorisierung	162
Übersicht über die -Sendeautorisierung	163

Sendeautorisierungsrichtlinien	165
Beispiele von Sendeautorisierungsrichtlinien	170
Aufgaben des Identitätseigentümers	175
Delegieren der Senderaufgaben	182
Verwenden dedizierter IP-Adressen	188
Einfache Einrichtung	189
Zuverlässigkeit durch AWS	190
Planbarkeit von Sendemustern	190
Volumen ausgehender E-Mails	190
Weitere Kosten	190
Kontrolle über die Senderreputation	191
Möglichkeit zur Isolierung der Reputation des Absenders	191
Bekannte, unveränderliche IP-Adressen	191
Beantragen und Freisetzen von dedizierten IP-Adressen	191
Aufwärmen dedizierter IPs	194
Erstellen von dedizierten IP-Pools	196
Eigene IP-Adressen mitbringen	197
Testen der E-Mail-Sendefunktion	198
Wichtige Überlegungen	198
Verwenden des Postfachsimulators	199
Testen von Reject-Ereignissen	200
Verwenden der Unterdrückungsliste auf Kontoebene	201
Überlegungen zur Unterdrückungsliste auf Kontoebene	201
Aktivieren der Unterdrückungsliste auf Kontoebene	202
Aktivieren der Unterdrückungsliste auf Kontoebene	202
Manuelles Hinzufügen von einzelnen E-Mail-Adressen zur Unterdrückungsliste auf Kontoebene ...	203
Massenanordnung von E-Mail-Adressen zur Unterdrückungsliste auf Kontoebene	204
Anzeigen einer Liste der Adressen, die sich in der Unterdrückungsliste auf Kontoebene befinden ..	205
Entfernen einer E-Mail-Adresse aus der Unterdrückungsliste auf Kontoebene	206
Entfernen einer Massenanordnung von E-Mails aus der Unterdrückungsliste auf Kontoebene	207
Anzeigen einer Liste der Importaufträge für das Konto	208
Abrufen von Informationen über einen Importauftrag für das Konto	209
Deaktivieren der Unterdrückungsliste auf Kontoebene	210
Verwenden der globalen Unterdrückungsliste in	210
Überlegungen zur globalen Unterdrückungsliste	210
Entfernen einer Adresse aus der globalen Unterdrückungsliste	211
Verwenden von Listenverwaltung	212
Übersicht über die Listenverwaltung	212
Konfigurieren der Listenverwaltung	212
Verwenden der Abonnementverwaltung	218
Übersicht über die Abonnementverwaltung	218
Hinzufügen eines Link zum Abmelden der Fußzeile	219
Überlegungen zur Abmeldung	219
Unterstützte Sicherheitsprotokolle	219
E-Mail-Absender an Amazon SES	219
Amazon SES an Empfänger	220
End-to-End-Verschlüsselung	220
Empfangen von E-Mails	222
Konzepte für den E-Mail-Empfang	222
Kontrolle auf der Grundlage des Empfängers	222
IP-adressbasierte Steuerung	223
E-Mail-Empfangsprozess	224
Erste Schritte: Empfangen von E-Mails	224
Schritt 1: Bevor Sie beginnen	225
Schritt 2: Überprüfen Ihrer Domäne	225
Schritt 3: So richten Sie eine Empfangsregel ein	226
Schritt 4: So senden Sie eine Test-E-Mail	228

Schritt 5: So zeigen Sie die E-Mail an	229
Schritt 6: Bereinigen	229
Einrichten des E-Mail-Empfangs in	230
Wenn Sie Ihren Anwendungsfall berücksichtigen	230
Überprüfen Ihrer Domäne	232
Veröffentlichen eines MX-Datensatzes	233
Erteilen einer Erlaubnis	235
Erstellen von IP-Adressenfilter	238
Erstellen eines Empfangsregel	238
Erstellen von Empfangsregeln	239
Verwalten des E-Mail-Empfangs	252
Verwalten von Empfangsregelsätzen	253
Verwalten von Empfangsregeln	255
Verwalten von IP-Adressfiltern	258
Anzeigen von Fehlermesriken	258
Verwenden von Benachrichtigungen	259
Verwenden von -Konfigurationssätzen	271
Verwalten von Konfigurationssätzen	271
Erstellen eines Konfigurationssatzes	271
Anzeigen einer Liste Ihrer Konfigurationssätze	272
Anzeigen der Details eines Konfigurationssatzes	273
Löschen eines Konfigurationssatzes	273
Verwalten von Standardkonfigurationssätzen	274
Verwalten von Ereigniszielen	277
Aktualisieren eines Ereignisziels	277
Löschen eines Ereignisziels	277
Aktivieren oder Deaktivieren eines Ereignisziels	278
Verwalten von IP-Pools	278
So weisen Sie einen IP-Pool einem Konfigurationssatz zu	278
Ändern von IP-Poolzuweisungen	279
Festlegen von Konfigurationssätzen in E-Mail	279
Exportieren von Zuverlässigkeitsmet	280
So aktivieren Sie den Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz	280
So deaktivieren Sie den Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz	280
Überwachen Ihrer -Sendeaktivität	282
Überwachen mithilfe der Konsole	284
Überwachen mithilfe der API	285
Aufrufen der API-Operation <code>GetSendStatistics</code> mithilfe der AWS CLI	285
Programmgesteuertes Aufrufen der Operation <code>GetSendStatistics</code>	286
Überwachen mit Benachrichtigungen	288
Wichtige Überlegungen	288
Benachrichtigungen per E-Mail	289
Amazon SNS Benachrichtigungen	292
Überwachen des Versands mithilfe der Ereignisveröffentlichung	313
Funktionsweise der -Ereignisveröffentlichung	313
Verwenden der Ereignisveröffentlichung	314
Terminologie zu Ereignisveröffentlichung	314
Einrichten der -Ereignisveröffentlichung	315
Arbeiten mit Ereignisdaten von	325
Tutorials	369
Überwachen Ihrer -Absenderzuverlässigkeit	400
Verwenden des Reputation Dashboards	400
Reputation Dashboard-Nachrichten	402
Allgemeine Statusnachrichten	402
Benachrichtigung zur Unzustellbarkeitsquote	403
Benachrichtigung zur Beschwerdequote	404
Benachrichtigungen zur Anti-Spam-Organisation	405

Benachrichtigungen zu direktem Feedback	406
Domain-Blocklist-Benachrichtigungen	407
Benachrichtigung zur internen Überprüfung	408
Benachrichtigung zum E-Mail-Dienstanbieter	410
Benachrichtigung zu Empfänger-Feedback	411
Benachrichtigung zu verknüpftem Konto	412
Benachrichtigung zu Pseudo-E-Mail-Adressen für Spam	412
Benachrichtigung zur Websiteanfälligkeit	413
Sonstige Benachrichtigung	414
Erstellen von Alarmen mit CloudWatch	415
SNDS-Metriken für dedizierte IP-Adressen	418
Fragen zur Fehlersuche	419
Automatisches Unterbrechen des E-Mail-Versands	419
Für Ihr gesamtes Konto	420
Für einen Konfigurationssatz	424
Steuern des Zugriffs	431
Erstellen von IAM-Richtlinien für den Zugriff auf Amazon SES	431
Beschränken der Aktion	432
Beschränken von E-Mail-Adressen	432
Beschränken der allgemeinen API-Nutzung	433
Beispielrichtlinien für Amazon SES	433
Berechtigen von Vollzugriff auf alle Amazon SES Aktionen	434
Erlauben von Zugriff nur auf Aktionen für den E-Mail-Versand	434
Beschränken des Sendezeitraums	434
Beschränken der Empfängeradressen	435
Beschränken der "From"-Adresse	435
Beschränken des Anzeigenamens des E-Mail-Absenders	436
Beschränken der Zieladresse des Unzustellbarkeits- und Beschwerde-Feedbacks	436
Protokollieren von API-Aufrufen	438
Amazon SES Informationen in CloudTrail	438
Beispiel: Amazon SES Protokolldateieinträge	440
Verwenden der API	442
API-Anfragen	442
Struktur einer GET-Anforderung	442
Struktur einer POST-Anforderung	443
Anforderungsauthentifizierung	444
Authentifizierungsfehler	445
GET- und POST-Beispiele	446
Beispiel für GET-Anforderung	446
Beispiel für POST-Anforderung	446
API-Antworten	447
Struktur einer erfolgreichen Antwort	447
Struktur einer Amazon SES Fehlerantwort	448
API-Fehlercodes	448
Codebeispiele	452
Senden von E-Mails mit AWS SDKs	452
Senden von E-Mails über die -SMTP-Schnittstelle	466
Senden von Raw-E-Mails mit AWS SDKs	478
Verifizieren mehrerer E-Mail-Adressen	487
Replizieren von Identitäten	488
Regionen	494
Amazon SES Regionen und -Endpunkte	494
Erhöhte Sandbox- und Sendelimits	495
Verifizierung von E-Mail-Adressen und Domains	495
Easy DKIM	495
Unterdrückungsliste	495
Feedback-Benachrichtigungen	495

SMTP-Anmeldeinformationen	496
Benutzerdefinierte MAIL FRO	496
Sendeautorisierung	497
Empfangen von E-Mails	497
Kontingente	499
E-Mail-Sendekontingente	499
Sendequote	499
Nachrichtenkontingente	499
Kontingente für Sender und Empfänger	500
Kontingente für die Ereignisveröffentlichung	500
Kontingente für E-Mail-Vorlagen	501
Kontingente für den E-Mail-Empfang	501
Allgemeine Kontingente	502
Amazon SES API-Kontingente	502
Bewährte Methoden	503
Erfolgsmetriken	503
Unzustellbarkeitsrate	503
Beschwerden	504
Nachrichtenqualität	505
Tipps und bewährte Methoden	506
Allgemeine Empfehlungen	506
Überlegungen zur Domäne und zur „From“-Adresse	506
Authentication	507
Erstellen und Pflegen von Listen	507
Compliance	507
Fehlersuche bei Amazon SES	508
Allgemeine Probleme	508
Änderungen, die ich vornehme, sind nicht direkt sichtbar	508
Verifizierungsprobleme	509
Probleme bei der E-Mail-Verifizierung	509
Probleme mit der Domänenverifizierung	509
Überprüfen der Einstellungen für die Domänenverifizierung	510
DKIM-Probleme	511
Zustellungsprobleme	513
Probleme mit empfangenen E-Mails	513
Benachrichtigungsprobleme	514
Fehler beim Senden von E-Mails	515
Erhöhen des Durchsatzes	517
SMTP-Probleme	518
SMTP-Antwortcodes	519
Löschen personenbezogener Daten	523
Löschen von unterdrückten Adressen	523
Löschen von Daten zu gesendeten E-Mails	524
Entfernen gespeicherter Ereignisdaten	524
Löschen von Daten über Identitäten	525
Löschen von Absender-Authentifizierungsdaten	525
Löschen von auf Empfangsregeln bezogenen Daten	526
Löschen von auf IP-Adressfilter bezogenen Daten	527
Löschen von Daten in E-Mail-Vorlagen	527
Löschen von Daten in benutzerdefinierten Vorlagen zur E-Mail-Verifizierung	527
Löschen aller Daten durch Schließen Ihres AWS Kontos	528
Häufig gestellte Fragen	529
Überprüfen	529
Konto wird geprüft	529
Sendeunterbrechungen	532
Unzustellbarkeit	534
Beschwerden	537

Pseudo-E-Mail-Adressen für Spam	542
Manuelle Überprüfungen	544
DNS-Blackhole-Liste (DNSBL)	546
DNSBL FAQ Q1	546
DNSBL FAQ Q2	547
DNSBL FAQ Q3	547
DNSBL FAQ Q4	547
DNSBL FAQ Q5	547
DNSBL FAQ Q6	548
E-Mail-Metriken	549
Allgemeines	549
Öffnungsnachverfolgung	550
Klicknachverfolgung	551
Ressourcen	553
Anhang	554
Header-Felder	554
Nicht-unterstützte Anhangtypen	556
Dokumentverlauf	557
.....	dlxii

Was ist Amazon SES?

Amazon SES Classic bezieht sich auf die ursprüngliche Amazon SES Konsole, APIs und Dokumentation, die für einen begrenzten Zeitraum verfügbar sind, bis sie veraltet sind. Dies ist das ursprüngliche SES-Entwicklerhandbuch, das jetzt als SES Classic Developer Guide bezeichnet wird. Diese Terminologieänderung soll das Original deutlicher von dem neuen Amazon SES Entwicklungshandbuch unterscheiden, der die neue Amazon SES-Konsole unterstützt.

Die neue Amazon SES Konsole ist jetzt mit verbesserten und leistungsfähigeren Funktionen wie Konfigurationsgruppen verfügbar, mit denen Sie alles, was Sie in Amazon SES Classic tun können, aber mit mehr Optionen, flexibler und effizienter Workflow. Einen schnellen Überblick über diese neuen Funktionen finden Sie unter [Amazon SES](#). Wir empfehlen Ihnen, diese Verbesserungen noch heute zu erkunden und zu nutzen, indem Sie die [Neue Amazon SES Konsole](#) und die [neue Amazon SES API \(bezeichnet als V2\)](#). Sie können über sie in der [neues Amazon SES Entwicklerhandbuch](#).

Amazon SES

[Amazon 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.

Für Amazon SES und das neue Amazon SES zahlen Sie nur für Ihre Nutzung. Weitere Informationen finden Sie unter [Amazon SES – Preise](#).

Warum Amazon SES verwenden?

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.

Amazon SES und andere AWS -Services

Amazon SES lässt sich reibungslos mit anderen AWS Produkten integrieren. Beispielsweise können Sie:

- Fähigkeiten zum Versenden von E-Mails zu jeder beliebigen Anwendung hinzufügen. Wenn Ihre Anwendung in [Amazon Elastic Compute Cloud](#) (Amazon EC2) können Sie Amazon SES verwenden, um [Senden Sie 62.000 E-Mails jeden Monat ohne zusätzliche Gebühren](#). Sie können E-Mails von

Amazon EC2 senden, indem Sie eine [AWS SDK](#), indem Sie die [Amazon SES — Schnittstelle \(p. 94\)](#), oder indem Sie direkt an die [Amazon SES API](#).

- Verwenden von [AWS Elastic Beanstalk](#) Verwenden Sie, um eine E-Mail-fähige Anwendung zu erstellen — z. B. ein Programm, das Amazon SES verwendet, um einen Newsletter an Kunden zu versenden.
- Einrichten [Amazon Simple Notification Service \(Amazon SNS\)](#) Richten Sie 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 die AWS Management Console, 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](#).
- 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 \(Amazon S3\)](#).
- Führen Sie über das Auslösen von [AWS Lambda](#)-Funktionen Aktionen für empfangene E-Mails aus.
- Verwenden von [AWS Key Management Service \(AWS KMS\)](#) Wenn Sie optional die E-Mails verschlüsseln, die Sie in Ihrem Amazon S3 Bucket erhalten.
- Verwenden von [AWS CloudTrail](#) Verwenden Sie, um Amazon SES API-Aufrufe zu protokollieren, die Sie über die Konsole oder die Amazon SES-API durchführen.
- Veröffentlichen Sie Ihre Versandereignisse an [Amazon CloudWatch](#) oder [Amazon Kinesis Data Firehose](#). Wenn Sie Ihre E-Mail-Versandereignisse in Kinesis Data Firehose veröffentlichen, können Sie diese über [Amazon Redshift](#), [Amazon Elasticsearch Service](#), oder [Amazon S3](#).

In diesem Handbuch

Dieses Handbuch enthält die folgenden Abschnitte:

Abschnitt	Beschreibung
Versand von E-Mails (p. 6)	Beschreibt, wie Sie mit Amazon SES E-Mails versenden können.
Empfangen von E-Mails (p. 222)	Beschreibt, wie Sie mit Amazon SES E-Mails empfangen können.
Steuern des Zugriffs (p. 431)	Beschreibt Ihnen, wie Sie Amazon SES mit AWS Identity and Access Management Verwenden Sie, um festzulegen, welche Amazon SES -API-Aktionen ein Benutzer mit welchen Amazon SES-Ressourcen durchführen kann.
Protokollieren von API-Aufrufen (p. 438)	Enthält eine Liste der Amazon SES APIs, die mit protokolliert werden können AWS CloudTrail .
Anmeldeinformationen (p. 18)	Beschreibt die Typen von Anmeldeinformationen, die Sie mit Amazon SES verwenden können, und wann Sie diese verwenden können.
Verwenden der API (p. 442)	Beschreibt die Interaktion mit der Amazon SES API.
Regionen (p. 494)	Enthält Informationen über die Verwendung von Amazon SES in mehreren AWS Regionen.
Kontingente (p. 499)	Enthält eine Liste der Kontingente, die für Amazon SES gelten.

Abschnitt	Beschreibung
Ressourcen (p. 553)	Führt Ressourcen auf, die bei der Arbeit mit Amazon SES hilfreich sind.
Anhang (p. 554)	Enthält zusätzliche Informationen über Header-Felder, nicht unterstützte Attachment-Typen und Skripte.

Amazon SES — Schnellstart

In diesem Verfahren werden die Schritte beschrieben, mit denen Sie sich bei AWS anmelden, Ihre E-Mail-Adresse verifizieren, die erste E-Mail senden, den Umgang mit unzustellbaren E-Mails und Beschwerden festlegen und die Sandbox von Amazon SES (Amazon SES) verlassen.

Verwenden Sie dieses Verfahren, wenn Folgendes auf Sie zutrifft:

- Sie möchten Amazon SES nur ausprobieren.
- Sie möchten einige Test-E-Mails senden, ohne programmieren zu müssen.
- Sie möchten die Ersteinrichtung mit möglichst wenigen Schritten vornehmen.

Schritt 1: Registrieren bei AWS

Bevor Sie Amazon SES nutzen können, müssen Sie sich bei AWS anmelden. Mit der AWS-Anmeldung wird Ihr Konto automatisch für alle AWS-Services registriert.

Detaillierte Anweisungen finden Sie unter [Registrieren bei AWS \(p. 51\)](#).

Schritt 2: Verifizieren Ihrer E-Mail-Adresse

Bevor Sie über Amazon SES E-Mails mit Ihrer E-Mail-Adresse senden können, müssen Sie Amazon SES den Besitz ihrer E-Mail-Adresse nachweisen, indem Sie diese verifizieren.

Detaillierte Anweisungen finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).

Schritt 3: Senden der ersten E-Mail

Sie können eine E-Mail ganz einfach über die Amazon SES Konsole senden. Da Sie ein neuer Benutzer sind, befindet sich Ihr Konto in einer als "Sandbox" bezeichneten Testumgebung, in der Sie E-Mails nur über Ihre verifizierten E-Mail-Adressen senden und empfangen können.

Detaillierte Anweisungen finden Sie unter [Senden einer E-Mail mit der Amazon SES Konsole \(p. 22\)](#).

Schritt 4: Überlegen Sie, wie Sie unzustellbare E-Mails und Beschwerden festlegen

Vor dem nächsten Schritt müssen Sie festlegen, wie Sie mit unzustellbaren E-Mails und Beschwerden umgehen möchten. Wenn Sie E-Mails an eine kleine Empfängergruppe senden, kann dieses Verfahren ganz einfach darin bestehen, das per E-Mail erhaltene Feedback in Bezug auf Unzustellbarkeiten und Beschwerden zu analysieren und die entsprechenden Empfänger dann aus Ihrer Mailing-Liste zu entfernen.

Schritt 5: Verlassen der Amazon SES -Sandbox

Damit Sie auch E-Mails an nicht verifizierte E-Mail-Adressen senden und die Anzahl der pro Tag gesendeten E-Mails sowie deren Sendegeschwindigkeit erhöhen können, muss Ihr Konto die Sandbox verlassen. In diesem Verfahren erstellen Sie ein SES-Verfahren im Support Center.

Weitere Informationen zu Sandbox-Einschränkungen und darüber, wie Sie das Verlassen der Sandbox beantragen, finden Sie unter [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

Nächste Schritte

- Bevor Sie sich einige Test-E-Mails senden, nutzen Sie dann den Amazon SES Postfachsimulator für weitere Tests — denn an den Postfachsimulator gesendete E-Mails werden nicht in Ihre Unzustellbarkeits- und Beschwerdequoten eingerechnet. Weitere Informationen zum Postfachsimulator finden Sie unter [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#).
- Überwachen Sie Ihre Sendeaktivität, wie z. B. die Anzahl der gesendeten E-Mails sowie die Anzahl der E-Mails, die unzustellbar sind oder für die Sie Beschwerden erhalten haben. Weitere Informationen finden Sie unter [Überwachen Ihrer Amazon SES Versandaktivitäten \(p. 282\)](#).
- Verifizieren Sie gesamte Domänen, damit Sie E-Mails von jeder E-Mail-Adresse in der Domäne senden können, ohne die einzelnen E-Mail-Adressen zu verifizieren. Weitere Informationen finden Sie unter [Überprüfen von Domänen in Amazon SES \(p. 65\)](#).
- Authentifizieren Sie Ihre E-Mails, um sicherzustellen, dass Ihre E-Mails im Posteingang der Empfänger landen (und nicht als Junk-E-Mails verworfen werden). Weitere Informationen finden Sie unter [Amazon Authentifizieren Ihrer E-Mails in Amazon SES \(p. 140\)](#).

Senden von E-Mails mit Amazon SES

Beim Senden von E-Mails wird ein Server für ausgehende E-Mails verwendet. Dieser E-Mail-Server wird von Ihrem Internetdienstanbieter (ISP), der IT-Abteilung Ihres Unternehmens oder von Ihnen selbst bereitgestellt. Der E-Mail-Server akzeptiert Ihren E-Mail-Inhalt, formatiert diesen den E-Mail-Standards entsprechend und sendet die E-Mail dann über das Internet. Die E-Mail wird möglicherweise über andere Server übertragen, bis sie bei einem Empfänger ankommt (eine Entität, wie eine ISP, die die E-Mail für den Empfänger erhält). Dieser Empfänger stellt die E-Mail dann dem endgültigen Empfänger zu. Das folgende Diagramm veranschaulicht den grundlegenden Ablauf zum Senden von E-Mail.



Wenn Sie Amazon SES verwenden, wird Amazon SES der Server für ausgehende E-Mail. Sie können Ihren vorhandenen E-Mail-Server auch beibehalten und ihn so konfigurieren, dass Ihre ausgehenden E-Mails über Amazon SES gesendet werden. So müssen Sie keine Einstellungen in Ihren E-Mail-Clients ändern. Im folgenden Diagramm wird beschrieben, wo sich Amazon SES in den Prozess zum Senden von E-Mail einfügt.



Ein Absender kann den E-Mail-Inhalt auf unterschiedliche Weise generieren. Ein Absender kann die E-Mail über eine E-Mail-Client-Anwendung erstellen oder ein Programm verwenden, das E-Mails automatisch generiert, wie eine Anwendung, die Auftragsbestätigungen beim Eintreten bestimmter Einkaufstransaktionen sendet.

Wie sende ich E-Mails mithilfe von Amazon SES?

Es gibt mehrere Möglichkeiten, wie Sie eine E-Mail mit Amazon SES senden können. Sie können die Amazon SES -Konsole oder die SMTP-Schnittstelle (Simple Mail Transfer Protocol) verwenden oder die Amazon SES -API aufrufen.

- **Amazon SES S-Konsole** Diese Methode bietet die schnellste Möglichkeit, um Ihr System einzurichten und eine Reihe von Test-E-Mails zu versenden. Sobald Sie jedoch bereit sind, Ihre E-Mail-Kampagne zu starten, verwenden Sie die Konsole in erster Linie zur Überwachung der Versandaktivität. Beispielsweise können Sie die Anzahl der E-Mails, die Sie gesendet haben, und die Anzahl der Unzustellbarkeitsnachrichten und Beschwerden, die Sie erhalten haben, auf einen Blick erkennen.
- **SMTP-Schnittstelle** Es gibt zwei Möglichkeiten, über die SMTP-Schnittstelle auf Amazon SES zuzugreifen. Die erste Möglichkeit, für die keine Codierung notwendig ist, ist, eine SMTP-fähige Software zum Senden von E-Mail über Amazon SES zu konfigurieren. Sie können beispielsweise Ihren vorhandenen E-Mail-Client oder ein entsprechendes Softwareprogramm konfigurieren, um eine Verbindung mit dem -SMTP-Endpunkt von Amazon SES und nicht mit dem aktuellen Server für ausgehende E-Mail herzustellen.

Die zweite Möglichkeit ist die Verwendung einer SMTP-kompatiblen Programmiersprache wie Java und der Zugriff auf die Amazon SES SMTP-Schnittstelle. Dabei nutzen Sie die integrierten SMTP-Funktionen und Datentypen der Programmiersprache.

- **Amazon SES** —Sie können die Amazon SES Query-API direkt über HTTPS aufrufen oder die [AWS Command Line Interface](#), die [AWS Tools for Windows PowerShell](#), oder ein [AWS SDK](#). Die AWS S-SDKs umschließen die Funktionen der Amazon SES -API auf niedriger Ebene mit Datentypen und Funktionsaufrufen der höheren Ebene, sodass Sie sich nicht um Details kümmern müssen. Die AWS S-SDKs bieten nicht nur Amazon SES S-Operationen, sondern auch grundlegende AWS Funktionen, wie Anforderungsauthentifizierung, wiederholte Anforderungsversuche und Fehlerbehandlung.

Wie beginne ich?

Wenn Sie noch nicht mit Amazon SES gearbeitet haben, lesen Sie zunächst die folgenden Abschnitte:

- [Amazon SES — Schnellstart \(p. 4\)](#) – Hier erfahren Sie, wie Sie sich einrichten und so schnell wie möglich eine Test-E-Mail senden.
- [Erste Schritte: Senden von E-Mails mit Amazon SES \(p. 21\)](#)— Hier erfahren Sie, wie Sie eine E-Mail mithilfe der Amazon SES -Konsole, der SMTP-Schnittstelle und einer AWS S-SDK senden. Beispiele sind in C#, Java und PHP verfügbar.
- [Amazon SES und Lieferbarkeit \(p. 8\)](#)— Hier werden die wichtigsten Konzepte zur E-Mail-Zustellbarkeit beschrieben. Mit diesen Konzepten sollten Sie vertraut sein, wenn Sie Amazon SES verwenden.
- [Amazon SES S-Prozess für den E-Mail-Versand \(p. 13\)](#)— Hier erfahren Sie, was passiert, wenn Sie eine E-Mail über Amazon SES senden.
- [E-Mail-Format und Amazon SES \(p. 16\)](#)— Überprüft das Format der E-Mails und identifiziert die Informationen, die Sie für Amazon SES bereitstellen müssen.

Anschließend können Sie mehr über das Senden von E-Mails mit Amazon SES erfahren, indem Sie die in der folgenden Tabelle aufgeführten Abschnitte lesen:

Abschnitt	Beschreibung
Einrichten von E-Mail (p. 50)	Hier erfahren Sie, wie Sie sich für AWS anmelden, Ihren AWS-Zugriffsschlüssel erhalten, ein AWS-SDK herunterladen, E-Mail-Adressen oder Domänen überprüfen und die Amazon SES -Sandbox verlassen.
Verwenden der SMTP-Schnittstelle (p. 94)	Hier erfahren Sie, wie Sie Ihre Amazon SES -SMTP-Anmeldeinformationen erhalten, eine Verbindung mit dem Amazon SES-SMTP-Endpunkt herstellen und sehen anhand von Beispielen, wie E-Mail-Clients und Softwarepakete zum Senden von E-Mails über Amazon SES konfiguriert werden. Außerdem wird erklärt, wie Sie Ihren bestehenden E-Mail-Server so konfigurieren, dass alle ausgehenden E-Mails über Amazon SES gesendet werden.
Verwenden der -API (p. 120)	Hier erfahren Sie, wie Sie formatierte oder Raw-E-Mails mithilfe der Amazon SES -API senden. Es wird erläutert, wie Sie Sonderzeichen verwenden und Anlagen senden, indem Sie den Multipurpose Internet Mail Extensions(MIME)-Standard nutzen, wenn Sie Raw-E-Mails senden.
E-Mail-Authentifizierungsmethoden (p. 140)	Hier erfahren Sie, wie Sie DKIM mit Amazon SES verwenden, um ISPs zu zeigen, dass Sie von Ihrer eigenen Domäne senden.

Abschnitt	Beschreibung
Verwalten von Sendekontingenten (p. 156)	Beschreibt die Amazon SES Sendekontingente, enthält Verfahren zum Erhöhen dieser Kontingente und dokumentiert die Fehler, die Sie erhalten, wenn Sie diese überschreiten.
Verwenden der Sendeautorisierung (p. 162)	Hier wird gezeigt, wie Sie andere Benutzer berechtigen, in Ihrem Namen E-Mails von Ihren Identitäten zu senden.
Verwenden dedizierter IP-Adressen (p. 188)	Sie entscheiden, ob Sie gemeinsame IP-Adressen verwenden oder dedizierte IP-Adressen für Ihre Amazon SES -Sendung leasen. Bietet Verfahren zum Beantragen und Freisetzen von dedizierten IPs und für die Erstellung von Pools dedizierter IPs.
Testen der E-Mail-Sendefunktion (p. 198)	Es wird erläutert, wie Sie den Amazon SES Postfachsimulator verwenden, um gängige E-Mail-Szenarien zu simulieren, ohne dass dies Auswirkungen auf Ihre Sendestatistiken hat, wie Ihre Metriken zu Unzustell Die Szenarien, die Sie testen können, sind eine erfolgreiche Zustellung, Unzustellbarkeit Beschwerden, Abwesenheitsnachricht und Adressen auf der Unterdrückungsliste.

Amazon SES S-Konzepte für den E-Mail-Versand

Die folgenden Abschnitte enthalten Informationen darüber, wie Amazon SES Ihre E-Mails sendet.

Themen in diesem Abschnitt:

- [Amazon SES und Lieferbarkeit \(p. 8\)](#)
- [Amazon SES S-Prozess für den E-Mail-Versand \(p. 13\)](#)
- [E-Mail-Format und Amazon SES \(p. 16\)](#)
- [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#)

Amazon SES und Lieferbarkeit

Sie möchten, dass Ihre Empfänger Ihre E-Mails lesen, sie als nützlich erachten und nicht als Spam einstufen. Mit anderen Worten: Sie möchten E-Mails maximieren Zustellbarkeit— Der Prozentanteil der E-Mails, die in den Posteingang Ihrer Empfänger eingehen. 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



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.

Bounce

Wenn der Receiver Ihres Empfängers (z. B. ein E-Mail-Anbieter) Ihre Nachricht dem Empfänger nicht zustellen kann, sendet er eine Unzustellbarkeitsnachricht an Amazon SES. Je nachdem, wie Ihr System eingerichtet ist, informiert Amazon SES Sie über die Unzustellbarkeitsnachricht per E-Mail oder über Amazon Simple Notification Service (Amazon SNS) über die Unzustellbarkeitsnachricht. Weitere Informationen finden Sie unter [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen](#) (p. 288) .

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

- Hartes Abprallen —Permanente E-Mail-Zustellungsfehler. Das Postfach ist beispielsweise nicht vorhanden. Mit Ausnahme von DNS-Suchfehlern versucht Amazon SES 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.

- **Weiche Unzustellbarkeit** Temporäre E-Mail-Zustellungsfehler. Wenn zum Beispiel das Postfach vollständig belegt ist, gibt es zu viele Verbindungen (und es kommt zur Ablehnung)-Ablehnung) oder die Zeitüberschreitung der Verbindung. Amazon SES führt bei wiederholter 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 ständige und vorübergehende 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 der `GetSendStatistics`-API.

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.

Complaint

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 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 [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen \(p. 288\)](#). Es wird ausdrücklich empfohlen, keine erneuten Zustellversuche an E-Mail-Adressen auszuführen, die zu Beschwerden führen.

Globale Unterdrückungsliste

Amazon SES Globale Unterdrückungsliste ist eine Liste der Empfänger-E-Mail-Adressen, die kürzlich eine harte Unzustellbarkeit für einen Amazon SES Kunden verursacht haben. Wenn Sie versuchen, eine E-Mail über Amazon SES an eine Adresse zu senden, die auf der Unterdrückungsliste steht, ist der Aufruf an Amazon SES erfolgreich, aber Amazon 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 eine Nachricht senden möchten, gültig ist, können Sie eine Anforderung zum Entfernen der Adresse aus der Unterdrückungsliste stellen. Weitere Informationen finden Sie unter [Verwenden der globalen Unterdrückungsliste von Amazon SES \(p. 210\)](#).

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

Verification

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 [Amazon Verifizieren von E-Mail-Adressen in Amazon SES](#) (p. 52) und [Überprüfen von Domänen in Amazon SES](#) (p. 65).

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 [Verlassen der Amazon SES -Sandbox](#) (p. 79). Weitere Informationen zum Postfachsimulator finden Sie unter [Testen der E-Mail-Versendung in Amazon SES](#) (p. 198).

Authentication

Die Authentifizierung 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 E-Mail-Anbieter die Weiterleitung von E-Mails, die nicht authentifiziert wurde. Amazon SES unterstützt zwei Authentifizierungsmethoden: Senderrichtlinie Framework (SPF) und DomainKeys Identified Mail (DKIM). Weitere Informationen finden Sie unter [Amazon Authentifizieren Ihrer E-Mails in Amazon SES](#) (p. 140).

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. Außerdem können Sie eine [Sending Limits Sending Limits Falls](#), um zusätzliche Kontingenterhöhungen anzufordern.

Weitere Informationen zu Sendekontingenten und dazu, wie sie erhöht werden, finden Sie unter [Verwalten Ihrer Amazon SES Versandkontingente](#) (p. 156).

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 zu bestimmen, ob Inhalte vorliegen, die von E-Mail-Anbietern als Spam eingestuft 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.

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

Reputation

Wenn es um das Senden von E-Mails geht, Zuverlässigkeit ist ein Maß für das Vertrauen darauf, dass eine IP-Adresse, E-Mail-Adresse oder sendende Domäne keinen Spam verursacht. Wenn Amazon SES gilt bei E-Mail-Anbietern als sehr zuverlässig, sodass Ihre E-Mails den Posteingang Ihrer Empfänger erreichen. Entsprechend müssen Sie vertrauenswürdige Zuverlässigkeit gegenüber Amazon SES zeigen. Sie fördern diese Zuverlässigkeit gegenüber Amazon SES, indem Sie hochwertige Inhalte senden. Wenn Sie hochwertige Inhalte senden, wird Ihre Zuverlässigkeit im Laufe der Zeit immer vertrauenswürdiger, sodass Amazon SES Ihre Sendekontingente erhöht. Übermäßige Unzustellbarkeiten und Beschwerden wirken sich negativ auf Ihre Zuverlässigkeit aus und können dazu veranlassen, dass Amazon SES die Sendekontingente für Ihr Konto reduziert oder Ihr Amazon SES-Konto beendet.

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 [Testen der E-Mail-Versendung in Amazon SES](#) (p. 198).

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 Amazon SES Ihnen dabei, das Problem zu ergründen, indem Benachrichtigungen und die Möglichkeit der Überwachung Ihrer Nutzungsstatistiken bereitgestellt werden.

Notifications

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 permanente Unzustellbarkeiten, bei denen Amazon SES keinen erneuten Zustellversuch mehr unternimmt. Viele E-Mail-Anbieter leiten Beschwerden außerdem weiter und Amazon SES richtet Feedback-Schleifen für Beschwerden für alle großen E-Mail-Anbieter ein, sodass Sie diesen Schritt nicht selbst ausführen müssen. Amazon SES kann Sie über Unzustellbarkeitsnachrichten, 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 Unzustellbarkeitsnachrichten und Beschwerden). Weitere Informationen finden Sie unter [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen](#) (p. 288).

Nutzungsstatistiken

Amazon SES statistiken, 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.

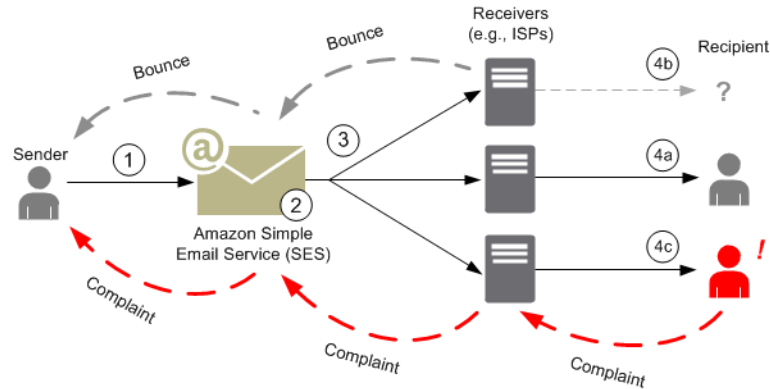
Verbessern Sie Ihr E-Mail-Programm

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 übermäßig viele

Unzustellbarkeitsnachrichten, Beschwerden und Versuche, geringwertige E-Mails zu senden, Missbrauch darstellen und Ihr AWS-Konto Gefahr läuft, geschlossen zu werden. 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.

Amazon SES S-Prozess für den E-Mail-Versand

In diesem Thema wird beschrieben, was geschieht, wenn Sie eine E-Mail mit Amazon 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 Amazon SES zum Senden von E-Mails an einen oder mehrere Empfänger.
2. Wenn die Anfrage gültig ist, akzeptiert Amazon SES die E-Mail.
3. Amazon SES sendet die Nachricht über das Internet an den Empfänger. Sobald die Nachricht an Amazon 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 Unzustellbarkeitsnachricht an Amazon SES sendet. Dann leitet Amazon SES die Benachrichtigung 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 Amazon SES eingerichtet hat, sendet die Beschwerde an Amazon 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 Amazon SES sendet und nachdem Amazon SES eine E-Mail-Nachricht an den Empfänger sendet.

Nach dem Senden einer E-Mail-Anforderung an Amazon SES

Wenn der Sender eine Anforderung zum Senden einer E-Mail an Amazon 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 Amazon SES erfolgreich, gibt Amazon 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 Mitteilungs-ID zum Identifizieren der gesendeten E-Mail oder zum Nachverfolgen der Probleme beim Senden verwenden. Amazon 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 Amazon SES die Anforderung des Senders akzeptiert und feststellt, dass die Nachricht einen Virus enthält, hält Amazon 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 Amazon SES des Senders fehlschlägt, reagiert Amazon 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 Amazon SES aufrufen. Im Folgenden finden Sie einige Beispiele dafür, wie Fehler und Ausnahmen zurückgegeben werden:

- Wenn Sie Amazon SES über die Abfrage (HTTPS) oder API (`SendEmail` oder `SendRawEmail`) zurück, geben die Aktionen einen Fehler zurück. Weitere Informationen finden Sie im [Amazon Simple Email Service API-Referenz](#).
- Wenn Sie ein AWS SDK für eine Programmiersprache verwenden, die Ausnahmen einsetzt, führt der Aufruf von Amazon SES zu einer `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 Amazon SES senden, finden Sie unter [Fehler beim Senden von Amazon SES E-Mails über](#) (p. 515).

Nachdem Amazon SES eine E-Mail gesendet hat

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

- Erfolgreiche Zustellung und der Empfänger widerspricht der E-Mail nicht —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.



- Harte Abprallung...Die E-Mail wird vom ISP aufgrund einer persistenten Bedingung abgelehnt oder sie wird von Amazon SES nicht akzeptiert, da sich die E-Mail-Adresse auf der Unterdrückungsliste von Amazon SES befindet. Eine E-Mail-Adresse befindet sich in der Unterdrückungsliste von Amazon SES, wenn sie kürzlich eine permanente Unzustellbarkeitsnachricht für einen Amazon SES -Kunden verursacht hat. Eine permanente Unzustellbarkeit durch einen ISP kann vorliegen, wenn die Adresse des Empfängers ungültig ist. Eine Benachrichtigung über die dauerhafte Unzustellbarkeit wird vom ISP zurück an Amazon 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. Amazon SES benachrichtigt den Sender über Unzustellbarkeiten aufgrund der

Unterdrückungsliste mit der gleichen Methode. Der Pfad einer permanenten Unzustellbarkeit für einen ISP ist in der folgenden Abbildung dargestellt.



- **Weiche Abprallung...** Aufgrund einer temporären Bedingung kann der ISP 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 Amazon SES oder im Falle einer nicht vorhandenen Domäne kann Amazon SES keinen E-Mail-Server für die Domäne finden. In beiden Fällen versucht Amazon SES über einen längeren Zeitraum, die E-Mail zuzustellen. Wenn Amazon SES die E-Mail in diesem Zeitraum nicht ausliefern kann, sendet es Ihnen eine Unzustellbarkeitsbenachrichtigung per E-Mail oder über Amazon SNS. Wenn Amazon SES die E-Mail bei einem der Wiederholungsversuche dem Empfänger zustellen kann, ist die Zustellung erfolgreich. Eine temporäre Unzustellbarkeit ist in der folgenden Abbildung dargestellt. In diesem Fall versucht Amazon SES wiederholt, die E-Mail zu senden, und der ISP ist schließlich in der Lage, sie dem Empfänger zuzustellen.



- **Complaint...** 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 Amazon SES eine Feedback-Schleife für den ISP eingerichtet hat, wird eine Beschwerdebenachrichtigung an Amazon SES gesendet, von wo sie an den Sender weitergeleitet wird. Da die meisten ISPs die E-Mail-Adresse des Empfängers, der sich beschwert hat, nicht offenlegen, stellt die Beschwerdebenachrichtigung von Amazon SES dem Sender eine Liste der Empfänger bereit, die sich beschwert haben könnten. Dabei basiert die Einschätzung auf den Empfängern der ursprünglichen E-Mail und dem ISP, von dem Amazon SES die Complaint. Der Pfad einer Beschwerde ist in der folgenden Abbildung dargestellt.



- **Auto Response** Der ISP akzeptiert die E-Mail und der ISP stellt sie dem Empfänger zu. Der ISP sendet dann eine automatische Antwort wie eine Abwesenheitsnachricht an Amazon SES. Amazon SES leitet die automatische Antwortbenachrichtigung an den Sender weiter. Eine automatische Antwort ist in der folgenden Abbildung dargestellt.



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

Tip

Sie können den Amazon 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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#).

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](#)) enthalten. 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 Mailserver während der SMTP-Sitzung ausgetauscht werden. Diese E-Mail-Umschlaginformationen sind vergleichbar mit den Informationen auf einem postalischen Umschlag. Die Weiterleitungsinformationen 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 Weiterleitungsinformationen 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 [Header-Felder \(p. 554\)](#). 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**...An diese E-Mail-Adresse werden Antworten gesendet. Standardmäßig werden die Antworten an die E-Mail-Adresse des ursprünglichen Senders gesendet.
- **Return-Path**...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. Für Empfänger, die textbasierte E-Mail-Clients verwenden, müssen Sie URLs einschließen, die sie kopieren und mit einem Webbrowser öffnen können.

E-Mail-Informationen, die Sie Amazon SES

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 mithilfe 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. 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-Client-Software optimiert ist. Weitere Informationen finden Sie unter [Senden von formatierten E-Mails mithilfe der Amazon SES API \(p. 121\)](#).
- 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 Raw-E-Mails mithilfe der Amazon SES API \(p. 121\)](#).

Wenn Sie die Amazon SES S-API mit einem AWS SDK aufrufen, geben Sie die oben aufgeführten Informationen für die entsprechenden Funktionen an (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 \(p. 120\)](#).

Amazon SES SMTP-Schnittstelle

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 eine Quelladresse, eine Zieladresse und Nachrichtendaten erforderlich. Wenn Sie die SMTP-Schnittstelle verwenden und die Weiterleitung von Feedback aktiviert ist, werden die Unzustellbarkeiten, Beschwerden und Zustellungsbenachrichtigungen an die "MAIL FROM"-Adresse gesendet. Jegliche "Reply-To"-Adressen, die Sie angeben, werden nicht verwendet.

Weitere Informationen zum Senden von E-Mails mit der -SMTP-Schnittstelle von Amazon SES finden Sie unter [Senden von E-Mails über die Amazon SES SMTP-Schnittstelle \(p. 94\)](#).

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. erstellt Amazon SES automatisch eine ordnungsgemäß formatierte mehrteilige MIME-E-Mail-Nachricht, die für die Darstellung mit E-Mail-Client-Software optimiert ist. Sie können auch ein 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.

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 mit der Amazon SES -API versenden, und SMTP-Anmeldeinformationen, wenn Sie eine E-Mail über die SMTP-Schnittstelle von Amazon SES 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 verwendende Anmeldeinformationen	Bestandteile der Anmeldeinformationen	Abrufen der Anmeldeinformationen
Amazon SES API (Sie können auf die Amazon SES S-API direkt zugreifen oder indirekt über ein AWS S-SDK, die AWS Command Line Interface, oder die AWS Tools for Windows PowerShell.)	AWS-Zugriffsschlüssel	Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	Siehe Zugriffsschlüssel im Allgemeinen AWS-Referenz. Note Für bewährte Sicherheitspraktiken verwenden Sie AWS Identity and Access Management Benutzerzugriffsschlüssel anstelle von AWS Konto-Zugriffsschlüsseln. Ihre Anmeldeinformationen für Ihr AWS Konto gewähren vollständigen Zugriff auf all Ihre AWS Ressourcen. Sie sollten sie daher an einem sicheren Ort speichern und für die täglichen Interaktionen mit AWS stattdessen IAM-Benutzeranmeldeinformationen verwenden. Weitere Informationen finden Sie unter Anmeldeinformationen für das Stammkonto und Anmeldeinformationen für IAM im Allgemeinen AWS-Referenz.
Amazon SES SMTP-Schnittstelle	SMTP-Anmeldeinformationen	Benutzername und Passwort	Siehe Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen (p. 95). Note Obwohl sich die -SMTP-Anmeldeinformationen von Ihren AWS Zugriffsschlüsseln und IAM-Benutzerzugriffsschlüsseln unterscheiden, sind Amazon SES SMTP-Anmeldeinformationen

Gewünschter Zugriff auf ...	Zu verwendende Anmeldeinformationen	Bestandteile der Anmeldeinformationen	Abrufen der Anmeldeinformationen
			tatsächlich eine Art von IAM-Anmeldeinformationen. Ein IAM-Benutzer kann -SMTP-Anmeldeinformationen erstellen, aber der Inhaber des Stammkontos muss sicherstellen, dass die Richtlinie für den IAM-Benutzer diesem Benutzer die Berechtigung gewährt, auf die folgenden IAM-Aktionen zuzugreifen: „iam:ListUsers“, „iam:CreateUser“, „iam:CreateAccessKey“ und „iam:PutUserPolicy“.
Amazon SES Konsole	IAM-Benutzername und -Passwort ODER E-Mail-Adresse und Passwort	IAM-Benutzername und -Passwort ODER E-Mail-Adresse und Passwort	Siehe IAM-Benutzername und -Passwort und E-Mail-Adresse und Passwort der Allgemeinen AWS-Referenz. Note Verwenden Sie als bewährte Sicherheitsmethode einen IAM-Benutzernamen und ein Passwort anstelle einer E-Mail-Adresse mit einem Passwort. Die Kombination aus E-Mail-Adresse und Passwort gilt für Ihr AWS-Konto, daher sollten Sie sie an einem sicheren Ort speichern und nicht für die täglichen Interaktionen mit AWS verwenden. Weitere Informationen finden Sie unter Anmeldeinformationen für das Stammkonto und Anmeldeinformationen für IAM in der Allgemeinen AWS-Referenz.

Weitere Informationen zu den verschiedenen Arten von AWS Anmeldeinformationen (außer SMTP-Anmeldeinformationen, die nur für Amazon SES verwendet werden) finden Sie unter [AWS Security Credentials](#) im Allgemeinen AWS-Referenz.

Erste Schritte: Senden von E-Mails mit Amazon SES

In diesem Tutorial „Erste Schritte“ finden Sie eine schrittweise Anleitung, mit der Sie Amazon Simple Email Service (Amazon SES) einrichten und eine E-Mail senden können. Lesen Sie zunächst die Informationen unter [Bevor Sie mit Amazon SES beginnen](#) (p. 21). Anschließend senden Sie eine E-Mail mit einer der folgenden Methoden.

Verwenden der Amazon SES Konsole

Mithilfe dieser Methode können Sie direkt und mit minimalem Konfigurationsaufwand Test-E-Mails über Amazon SES senden. Wenn Sie jedoch eine E-Mail-Produktionskampagne starten möchten, sollten Sie eine der anderen Sendemethoden einsetzen und die Amazon SES Konsole in erster Linie zum Überwachen der Sendeaktivität nutzen.

Rufen Sie [Senden einer E-Mail mit der Amazon SES Konsole](#) (p. 22) auf, um mit diesem Tutorial zu beginnen.

Verwenden von SMTP (Simple Mail Transfer Protocol)

Mit dieser Methode können Sie wie folgt E-Mails über die Amazon SES SMTP-Schnittstelle (mit oder ohne Programmierung) senden:

- Aktivieren Sie eine Anwendung mithilfe einer Programmiersprache, die SMTP unterstützt, zum Senden von E-Mails über Amazon SES. Beispiele sind in C#, Java und PHP verfügbar. Rufen Sie [Programmatisches Senden einer E-Mail über die Amazon SES -SMTP-Schnittstelle](#) (p. 24) auf, um mit diesem Tutorial zu beginnen.
- Richten Sie den E-Mail-Server so ein, dass die E-Mails an Amazon SES weitergeleitet werden. Alternativ können Sie den E-Mail-Client oder das SMTP-fähige Softwarepaket so konfigurieren, dass E-Mails über Amazon SES gesendet werden. Beispiele sind für die Mail-Server Postfix, Sendmail und angegeben. Rufen Sie [Konfigurieren Ihres vorhandenen E-Mail-Servers oder Ihrer SMTP-fähigen Anwendung für das Senden von E-Mails über Amazon SES](#) (p. 33) auf, um mit diesem Tutorial zu beginnen.

Einführende Informationen zu beiden SMTP-Sendemethoden finden Sie unter [So senden Sie mit SMTP eine E-Mail über Amazon SES](#) (p. 23).

Verwenden eines AWS SDK

Mit dieser Methode rufen Sie die Amazon SES API — unter Verwendung von Bibliotheken für die Detailverarbeitung der zugrunde liegenden Amazon SES-Abfrageschnittstelle — auf. Beispiele sind in C#, Java, PHP, Ruby und Python verfügbar. Rufen Sie [Senden einer E-Mail über Amazon SES mithilfe eines AWS -SDKs](#) (p. 34) auf, um mit diesem Tutorial zu beginnen.

Bevor Sie mit Amazon SES beginnen

Bevor Sie beginnen, müssen Sie Amazon SES einrichten. Unabhängig davon, ob Sie eine E-Mail über die Amazon SES Konsole, die SMTP-Schnittstelle oder die Amazon SES-API senden möchten, sind folgende Schritte erforderlich:

- Registrieren bei AWS —Sie müssen ein AWS Konto einrichten, ehe Sie auf Amazon SES oder andere AWS-Services zugreifen können. Weitere Informationen finden Sie unter [Registrieren bei AWS](#) (p. 51).
- Überprüfen Sie Ihre E-Mail-Adresse oder Domäne —Um E-Mails mit Amazon SES senden zu können, müssen Sie immer den Besitz ihrer E-Mails nachweisen. Falls Sie sich in einer Sandbox-Umgebung befinden, müssen auch die Empfängeradressen verifiziert werden. Sie können E-Mail-Adressen oder ganze Domänen verifizieren. Weitere Informationen finden Sie unter [Überprüfen von Identitäten in Amazon SES](#) (p. 52).
- Geben Sie Ihre Kontodaten an...Halten Sie Ihr Konto auf dem neuesten Stand, indem Sie Ihre Kontodetails bearbeiten. Wenn Sie Ihre Kontodaten angeben, können Sie auch beantragen, aus der Sandbox zu wechseln. Wenn Sie sich in der Sandbox befinden, können Sie nur E-Mails an den Amazon SES Postfachsimulator und verifizierte E-Mail-Adressen oder Domänen senden. Weitere Informationen finden Sie unter [Verlassen der Amazon SES -Sandbox](#) (p. 79).

Diese Liste enthält die Setup-Aufgaben, die für alle E-Mail-Sendemethoden ausgeführt werden müssen. Die zusätzlichen Setup-Aufgaben für die einzelnen E-Mail-Sendemethoden finden Sie im jeweiligen Abschnitt "Erste Schritte". Eine vollständige Liste aller Setup-Aufgaben finden Sie unter [Einrichten von E-Mail mit Amazon SES](#) (p. 50).

Senden einer E-Mail mit der Amazon SES Konsole

Die einfachste Möglichkeit, um eine E-Mail mit Amazon SES zu senden, ist die Amazon SES-Konsole. 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 Amazon SES senden Sie Ihre E-Mails wahrscheinlich entweder über die Amazon SES SMTP-Schnittstelle oder -API. Die Konsole ist jedoch praktisch, um Ihre Sendeaktivität zu überwachen.

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 [Testen der E-Mail-Versendung in Amazon SES](#) (p. 198) .

Bevor Sie diese Schritte ausführen, lesen Sie bitte die Installationsanweisungen unter [Bevor Sie mit Amazon SES beginnen](#) (p. 21).

So senden Sie eine E-Mail-Nachricht über die Amazon SES Konsole aus

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.

Note

Wenn Sie zurzeit nicht bei Ihrem AWS Konto angemeldet sind, ruft dieser Link eine Anmeldeseite auf. Nachdem Sie sich angemeldet haben, werden Sie zur Amazon SES Konsole weitergeleitet.

2. Klicken Sie im Navigationsbereich auf der linken Seite der Amazon SES Konsole unterIdentitätsmanagement, wählen SieE-Mail-AdressenÜberprüfen Sie, ob die E-Mail-Adresse, die Sie in überprüft haben[Amazon Verifizieren von E-Mail-Adressen in Amazon SES](#) (p. 52).
3. Aktivieren Sie in der Liste der Identitäten das Kontrollkästchen neben der E-Mail-Adresse, die Sie verifiziert haben.
4. Wählen Sie Send a Test Email aus.
5. Wählen Sie in Send Test Email Email Format aus. Folgende beiden Optionen sind verfügbar:

- **Formatiert** 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 Raw-E-Mails mithilfe der Amazon SES API \(p. 121\)](#) 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. Füllen Sie für Send Test Email die restlichen Felder aus. Wenn Sie noch immer in der Amazon SES -Sandbox sind, stellen Sie sicher, dass die Adresse im `Bis`-Feld ist eine verifizierte E-Mail-Adresse. Weitere Informationen finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
7. Wählen Sie Send Test Email aus.
8. 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.

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

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, lesen Sie die Anweisungen in [Bevor Sie mit Amazon SES beginnen \(p. 21\)](#). Außerdem benötigen Sie die folgenden zusätzlichen Informationen:

- Ihren Amazon SES SMTP-Benutzername und das Passwort, mit denen Sie sich mit dem Amazon SES -SMTP-Endpunkt verbinden können. Informationen zum Abrufen Ihres Amazon SES Benutzernamens und Ihres Passworts finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#).

Important

Ihre SMTP-Anmeldeinformationen sind nicht mit den AWS-Anmeldeinformationen identisch. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#).

- Die SMTP-Endpunktadresse. Eine Liste der Amazon SES SMTP-Endpunkte finden Sie unter [Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt \(p. 100\)](#).

- Die Portnummer der -SMTP-Schnittstelle von Amazon SES. Diese hängt von der Verbindungsmethode ab. Weitere Informationen finden Sie unter [Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt \(p. 100\)](#) .

Nachdem Sie Ihre SMTP-Anmeldeinformationen erhalten haben, können Sie sich mit dem Amazon SES SMTP-Endpunkt verbinden und E-Mails versenden. Dieses Tutorial zeigt Ihnen, wie Sie mit den folgenden Methoden E-Mails über die Amazon SES SMTP-Schnittstelle versenden können:

- [Programmatisches Senden einer E-Mail über die Amazon SES -SMTP-Schnittstelle \(p. 24\)](#)
- [Konfigurieren Ihres vorhandenen E-Mail-Servers oder Ihrer SMTP-fähigen Anwendung für das Senden von E-Mails über Amazon SES \(p. 33\)](#)

Weitere Informationen über die Amazon SES SMTP-Schnittstelle finden Sie unter [Senden von E-Mails über die Amazon SES SMTP-Schnittstelle \(p. 94\)](#).

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

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

Note

Standardmäßig beschränkt Amazon Elastic Compute Cloud (Amazon EC2) den E-Mail-Verkehr über Port 25. Um Zeitüberschreitungen beim Versenden 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 Einschränkung auf Port 25 von meiner Amazon EC2 Instance oder der AWS Lambda Funktion?](#) im AWS-Wissenszentrum. Die Codebeispiele in diesem Abschnitt verwenden Port 587, um dieses Problem zu vermeiden.

Themen in diesem Abschnitt:

- [Senden einer E-Mail per SMTP mit C# \(p. 24\)](#)
- [Senden einer E-Mail über SMTP mit Java \(p. 27\)](#)
- [Senden einer E-Mail mittels SMTP mit PHP \(p. 30\)](#)

Senden einer E-Mail per SMTP mit C#

Im folgenden Verfahren wird beschrieben, wie [Microsoft Visual Studio](#) Erstellen Sie eine C#-Konsolenanwendung, die eine E-Mail über Amazon SES sendet. Die Prozeduren in diesem Abschnitt gelten für Visual Studio 2017, aber der Prozess der Erstellung von C#-Konsolenanwendungen ist in allen Microsoft Visual Studio-Editionen ähnlich.

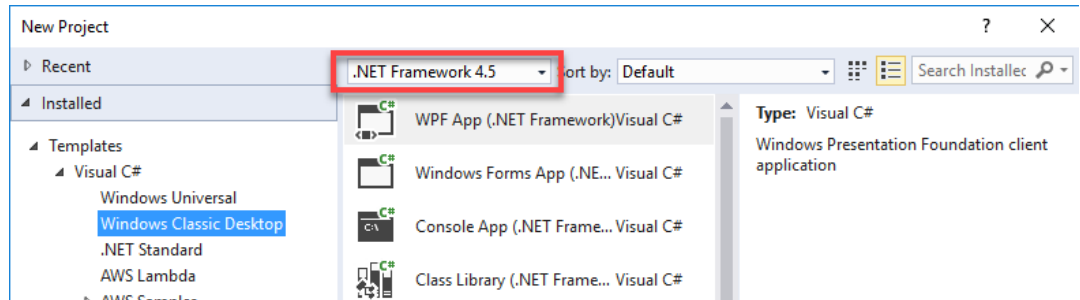
Führen Sie erst die unter [Bevor Sie mit Amazon SES beginnen \(p. 21\)](#) und [So senden Sie mit SMTP eine E-Mail über Amazon SES \(p. 23\)](#) beschriebenen Setup-Aufgaben aus, bevor Sie mit dem folgenden Verfahren beginnen.

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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#) .

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

1. Erstellen Sie ein Konsolenprojekt in Visual Studio, indem Sie die folgenden Schritte ausführen:
 - a. Öffnen Sie Microsoft Visual Studio.
 - b. Wählen Sie im Menü Datei Neu, Projekt aus.
 - c. Erweitern Sie im linken Bereich des Fensters Neues Projekt die Einträge Installiert, Vorlagen und Visual C#.
 - d. Wählen Sie unter Visual C# die Option Windows Classic Desktop.
 - e. Wählen Sie im Menü am oberen Rand des Fensters die Option .NET Framework 4.5, wie in der folgenden Abbildung gezeigt.



Note

Sie können bei Bedarf eine spätere Version des .NET Frameworks auswählen.

- f. Wählen Sie Konsolenanwendung (.NET Framework) aus.
 - g. Geben Sie in das Name-Feld AmazonSESSample ein.
 - h. Klicken Sie auf OK.
2. Ersetzen Sie in Ihrem Visual Studio-Projekt den gesamten Inhalt von Program.cs durch den folgenden Code:

```
using System;
using System.Net;
using System.Net.Mail;

namespace AmazonSESSample
{
    class Program
    {
        static void Main(string[] args)
        {
            // Replace sender@example.com with your "From" address.
            // This address must be verified with Amazon SES.
            String FROM = "sender@example.com";
            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.
            String TO = "recipient@amazon.com";

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

            // Replace smtp_password with your Amazon SES SMTP password.
            String SMTP_PASSWORD = "smtp_password";

            // (Optional) the name of a configuration set to use for this message.
            // If you comment out this line, you also need to remove or comment out
            // the "X-SES-CONFIGURATION-SET" header below.
```

```
String CONFIGSET = "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 AWS Region.
String HOST = "email-smtp.us-west-2.amazonaws.com";

// The port you will connect to on the Amazon SES SMTP endpoint. We
// are choosing port 587 because we will use STARTTLS to encrypt
// the connection.
int PORT = 587;

// The subject line of the email
String SUBJECT =
    "Amazon SES test (SMTP interface accessed using C#)";

// The body of the email
String BODY =
    "<h1>Amazon SES Test</h1>" +
    "<p>This email was sent through the " +
    "<a href='https://aws.amazon.com/ses'>Amazon SES</a> SMTP interface " +
    "using the .NET System.Net.Mail library.</p>";

// Create and build a new MailMessage object
MailMessage message = new MailMessage();
message.IsBodyHtml = true;
message.From = new MailAddress(FROM, FROMNAME);
message.To.Add(new MailAddress(TO));
message.Subject = SUBJECT;
message.Body = BODY;
// Comment or delete the next line if you are not using a configuration set
message.Headers.Add("X-SES-CONFIGURATION-SET", CONFIGSET);

using (var client = new System.Net.Mail.SmtpClient(HOST, PORT))
{
    // Pass SMTP credentials
    client.Credentials =
        new NetworkCredential(SMTP_USERNAME, SMTP_PASSWORD);

    // Enable SSL encryption
    client.EnableSsl = true;

    // Try to send the message. Show status in console.
    try
    {
        Console.WriteLine("Attempting to send email...");
        client.Send(message);
        Console.WriteLine("Email sent!");
    }
    catch (Exception ex)
    {
        Console.WriteLine("The email was not sent.");
        Console.WriteLine("Error message: " + ex.Message);
    }
}
}
```

3. Ersetzen Sie in Program.cs 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 dies durch Ihre Absender-E-Mail-Adresse. Sie müssen diese Adresse verifizieren, bevor Sie das Programm ausführen. Weitere Informationen finden Sie unter [Überprüfen von Identitäten in Amazon SES \(p. 52\)](#) .
 - `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 [Verlassen der Amazon SES -Sandbox \(p. 79\)](#) .
4. Ersetzen Sie in `Program.cs` die folgenden SMTP-Anmeldeinformationen durch die Werte, die Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#) abgerufen haben:
- Important
- Ihre SMTP-Anmeldeinformationen sind nicht mit den AWS-Anmeldeinformationen identisch. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#).
- `YOUR_SMTP_USERNAME` – Ersetzen Sie dies mit Ihrem SMTP-Benutzernamen. Beachten Sie, dass der SMTP-Benutzername eine 20-stellige Zeichenfolge aus Buchstaben und Zahlen ist und kein wirklicher Name.
 - `YOUR_SMTP_PASSWORD` – Ersetzen Sie dies mit Ihrem SMTP-Passwort.
5. (Optional) — Wenn Sie einen Amazon SES SMTP-Endpunkt in einer anderen Region als US West (Oregon) verwenden möchten, ändern Sie den Wert der Variable `HOST` auf den Endpunkt, den Sie verwenden möchten. Eine Liste der SMTP-Endpunkt-URLs für die AWS Regionen, in denen Amazon SES verfügbar ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeine AWS-Referenz.
6. (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 \(p. 271\)](#).
7. Speichern `Program.cs`.
8. Wählen Sie zum Erstellen des Projekts Erstellen und dann Lösung erstellen aus.
9. Um das Programm auszuführen, wählen Sie Debuggen und anschließend Debuggen starten aus.
10. Überprüfen Sie die Ausgabe. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole "Email sent!" an. Andernfalls wird eine Fehlermeldung angezeigt.
11. Melden Sie sich am E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

Senden einer E-Mail über SMTP mit Java

In diesem Beispiel verwenden wir den [Eclipse IDE](#) und die [JavaMail API](#) zum Senden von E-Mails über Amazon SES über die SMTP-Schnittstelle verwenden.

Führen Sie erst die unter [Bevor Sie mit Amazon SES beginnen \(p. 21\)](#) und [So senden Sie mit SMTP eine E-Mail über Amazon SES \(p. 23\)](#) beschriebenen Setup-Aufgaben aus, bevor Sie mit dem folgenden Verfahren beginnen.

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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#) .

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

1. Rufen Sie in einem Webbrowser die Seite [JavaMail Github](#) auf. Wählen Sie unter Downloads die Option `javax.mail.jar` aus, um die neueste JavaMail-Version herunterzuladen.

Important

Für dieses Tutorial ist die JavaMail-Version 1.5 oder höher erforderlich. Diese Schritte wurden mit JavaMail Version 1.6.1 getestet.

2. Erstellen Sie ein Projekt in Eclipse, indem Sie die folgenden Schritte ausführen:
 - a. Starten Sie Eclipse.
 - b. Wählen Sie in Eclipse die Optionen File, New und dann Java Project aus.
 - c. Geben Sie im Dialogfeld Create a Java Project einen Projektnamen ein und klicken Sie auf Next.
 - d. Wählen Sie im Dialogfeld Java Settings die Registerkarte Libraries aus.
 - e. Klicken Sie auf Add External JARs.
 - f. Navigieren Sie zu dem Ordner, in den Sie JavaMail heruntergeladen haben. Wählen Sie die Datei `javax.mail.jar` und dann Open aus.
 - g. Klicken Sie im Dialogfeld Java Settings auf Finish.
3. Erweitern Sie im Eclipse-Fenster Package Explorer das Projekt.
4. Klicken Sie unter Ihrem Projekt mit der rechten Maustaste auf das Verzeichnis `src` und wählen Sie New und dann Class aus.
5. Geben Sie im Dialogfeld New Java Class im Feld Name die Zeichenfolge `AmazonSESSample` ein und klicken Sie auf Finish.
6. Ersetzen Sie den gesamten Inhalt von `AmazonSESSample.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";

    // Replace smtp_password with your Amazon SES SMTP password.
    static final String SMTP_PASSWORD = "smtp_password";

    // 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();

    // 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();
    }
}
```

```
}  
}
```

7. Ersetzen Sie in `AmazonSESSample.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 dies durch Ihre Absender-E-Mail-Adresse. Sie müssen diese Adresse verifizieren, bevor Sie das Programm ausführen. Weitere Informationen finden Sie unter [Überprüfen von Identitäten in Amazon SES \(p. 52\)](#).
- `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 [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

8. Ersetzen Sie in `AmazonSESSample.java` die folgenden SMTP-Anmeldeinformationen durch die Werte, die Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#) abgerufen haben:

Important

Ihre SMTP-Anmeldeinformationen sind nicht mit den AWS-Anmeldeinformationen identisch. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#).

- `YOUR_SMTP_USERNAME`– Ersetzen Sie dies durch Ihren SMTP-Benutzernamen. Beachten Sie, dass der SMTP-Benutzername eine 20-stellige Zeichenfolge aus Buchstaben und Zahlen ist und kein wirklicher Name.
 - `YOUR_SMTP_PASSWORD` – Ersetzen Sie dies durch Ihr SMTP-Passwort.
9. (Optional) — Wenn Sie einen Amazon SES SMTP-Endpunkt in einer anderen AWS Region als US West (Oregon) verwenden möchten, ändern Sie den Wert der Variable `HOST` auf den Endpunkt, den Sie verwenden möchten. Eine Liste der Regionen, in denen Amazon SES erhältlich ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen AWS-Referenz.
10. (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 \(p. 271\)](#).
11. Speichern `AmazonSESSample.java`.
12. Wählen Sie Project (Projekt) und dann Build Project (Build-Projekt) aus. (Falls diese Option deaktiviert ist, kann die automatische Erstellung aktiviert sein.)
13. Wählen Sie Run und dann erneut Run aus, um das Programm zu starten und die E-Mail zu senden.
14. Überprüfen Sie die Ausgabe. Wenn die E-Mail erfolgreich gesendet wurde, zeigt die Konsole "Email sent!" an. Andernfalls wird eine Fehlermeldung angezeigt.
15. Melden Sie sich am E-Mail-Client der Empfängeradresse an. Sie finden die Nachricht, die Sie gesendet haben.

Senden einer E-Mail mittels SMTP mit PHP

In diesem Beispiel wird die PHPMailer-Klasse zum Senden von E-Mails über Amazon SES mit der SMTP-Schnittstelle verwendet.

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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#).

Prerequisites

Führen Sie vor Beginn die folgenden Schritte durch:

- Amazon Simple Email Service— Bevor Sie E-Mails mit Amazon 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. Dies lässt sich am einfachsten mit der Amazon SES Konsole durchführen. Weitere Informationen finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
- Abrufen Ihrer SMTP-Anmeldeinformationen— Sie benötigen einen Amazon SES SMTP-Benutzernamen und ein Passwort für den Zugriff auf die Amazon SES SMTP-Schnittstelle. Ihre SMTP-Anmeldeinformationen sind nicht so wie Ihre AWS Anmeldeinformationen. Sie finden Ihre SMTP-Anmeldeinformationen unter [SMTP-Einstellungen](#) der Amazon SES Konsole. Weitere Informationen zu SMTP-Anmeldeinformationen finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#).
- Installieren von PHP— PHP finden Sie unter <http://php.net/downloads.php>. Fügen Sie nach der Installation von PHP Ihren Umgebungsvariablen den Pfad zu PHP hinzu, damit Sie PHP von jeder Eingabeaufforderung aus ausführen können.
- Installieren des Composer-Abhängigkeits-Managers— Der Composer-Abhängigkeitsmanager ermöglicht Ihnen das Herunterladen und Installieren der PHPMailer-Klasse mit den dazugehörigen Abhängigkeiten. Befolgen Sie die Anleitung unter <https://getcomposer.org/download>, um den Composer zu installieren.
- PHPMailer-Klasse installieren— Nachdem Sie Composer installiert haben, führen Sie den folgenden Befehl aus, um PHPMailer zu installieren:

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

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

Procedure

Im folgenden Verfahren wird beschrieben, wie Sie mit PHP eine E-Mail über Amazon SES senden.

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

1. Erstellen Sie eine Datei namens `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';

// Replace smtp_password with your Amazon SES SMTP password.
$passwordSmtp = 'smtp_password';

// 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 = $passwordSmtp;
    $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.
}
```



```
?>
```

2. Ersetzen Sie in `amazon-ses-smtp-sample.php` 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 [Verifizieren von Identitäten \(p. 52\)](#). Bei 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 [Verlassen der Amazon SES -Sandbox \(p. 79\)](#). Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
 - **smtp_username**— Ersetzen Sie dies durch Ihren SMTP-Benutzernamen, den Sie über das [SMTP-Einstellungen](#) der Amazon SES Konsole. Das ist nicht genauso wie Ihre AWS Zugriffsschlüssel-ID. Beachten Sie, dass der SMTP-Benutzername eine 20-stellige Zeichenfolge aus Buchstaben und Zahlen ist und kein wirklicher Name.
 - **smtp_password**— Ersetzen Sie diesen Wert durch Ihr SMTP-Passwort, das Sie über die [SMTP-Einstellungen](#) der Amazon SES Konsole. Das ist nicht wie Ihr geheimer AWS Zugriffsschlüssel.
 - (Optional) **ConfigSet**— Wenn Sie beim Senden dieser E-Mail einen Konfigurationssatz senden möchten, ersetzen Sie diesen Wert durch den Namen des Konfigurationssatzes. Weitere Informationen zu Konfigurationssätzen finden Sie unter [Verwenden von Amazon SES Konfigurationssätzen \(p. 271\)](#).
 - (Optional) **email-smtp.us-west-2.amazonaws.com**— Wenn Sie einen Amazon SES SMTP-Endpunkt in einer anderen Region als USA West (Oregon) verwenden möchten, ersetzen Sie diese Angabe durch den Amazon SES-SMTP-Endpunkt für die gewünschte Region. Eine Liste der SMTP-Endpunkt-URLs für die AWS Regionen, in denen Amazon SES verfügbar ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen AWS-Referenz.
3. Speichern `amazon-ses-smtp-sample.php`.
4. Um das Programm zu starten, öffnen Sie eine Eingabeaufforderung in demselben Verzeichnis wie `amazon-ses-smtp-sample.php` und geben Sie `php amazon-ses-smtp-sample.php` 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.

Konfigurieren Ihres vorhandenen E-Mail-Servers oder Ihrer SMTP-fähigen Anwendung für das Senden von E-Mails über Amazon SES

Sie können Ihren Mailserver, Ihren E-Mail-Client oder Ihr E-Mail-Versand-Softwarepaket so konfigurieren, dass Sie Nachrichten über Amazon SES ohne jegliche Programmierung versenden können.

Lesen Sie zuerst [So senden Sie mit SMTP eine E-Mail über Amazon SES \(p. 23\)](#). Lesen Sie dann eines der folgenden Themen. Diese zeigen Ihnen, wie Sie einen Mailserver so konfigurieren, dass er E-Mails an Amazon SES weiterleitet:

- [Konfigurieren von Postfix \(p. 103\)](#)
- [Integrieren von Amazon SES mit Sendmail \(p. 106\)](#)
- [Integration von Amazon SES mit Exim \(p. 111\)](#)

Senden einer E-Mail über Amazon SES mithilfe eines AWS -SDKs

Zum Senden einer E-Mail mit der Amazon SES S-API können Sie die Abfrageschnittstelle direkt verwenden oder ein AWS SDK nutzen, um Details der unteren Ebene, wie beispielsweise das Zusammenstellen und Analysieren von HTTP-Anforderungen und -Antworten, einzusetzen.

Lesen Sie die Anleitungen unter, ehe Sie eine E-Mail mit einem AWS S-SDK senden. [Bevor Sie mit Amazon SES beginnen \(p. 21\)](#). Um die Tutorials in diesem Abschnitt abzuschließen, müssen Sie zudem Folgendes durchführen:

- Herunterladen eines AWS-SDK— Laden Sie ein AWS SDK herunter und installieren Sie es. Weitere Informationen finden Sie unter [Herunterladen eines AWS SDKs \(p. 72\)](#).
- Abrufen Ihrer AWS Anmeldeinformationen auf Amazon SES zugreifen können, benötigen Sie AWS Zugriffsschlüssel. Weitere Informationen finden Sie unter [Abrufen von AWS-Zugriffsschlüsseln \(p. 71\)](#).
- Erstellen einer gemeinsamen Anmeldeinformationsdatei – Führen Sie die unter [Erstellen einer freigegebenen Anmeldeinformationsdatei \(p. 34\)](#) beschriebenen Schritte durch, um eine gemeinsame Anmeldeinformationsdatei zu erstellen.

Wenn Sie die oben genannten Voraussetzungen erfüllt haben, lesen Sie [Programmgesteuertes Senden einer E-Mail über Amazon SES mithilfe eines AWS SDK \(p. 35\)](#).

Erstellen einer freigegebenen Anmeldeinformationsdatei

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 gerade von Ihnen erstellten Textdatei `YOUR_AWS_ACCESS_KEY_ID` durch Ihre eindeutige AWS Zugriffsschlüssel-ID und `YOUR_AWS_SECRET_ACCESS_KEY` mit Ihrem einzigartigen geheimen AWS 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.

Programmgesteuertes Senden einer E-Mail über Amazon SES mithilfe eines AWS SDK

Sie können ein AWS -SDK zum Senden von E-Mails über Amazon SES verwenden. AWS SDKs sind für mehrere Programmiersprachen verfügbar. Weitere Informationen finden Sie unter [Tools für Amazon Web Services](#).

Note

Wenn Sie es nicht bereits getan haben, stellen Sie sicher, dass die unter [Senden einer E-Mail über Amazon SES mithilfe eines AWS -SDKs \(p. 34\)](#) aufgeführten Voraussetzungen erfüllt sind, bevor Sie versuchen, die Tutorials in diesem Abschnitt durchzuarbeiten.

Weitere Codebeispiele finden Sie unter [Amazon SES Codebeispiele \(p. 452\)](#).

Themen in diesem Abschnitt:

- [Senden einer E-Mail mit dem AWS SDK for .NET \(p. 35\)](#)
- [Senden einer E-Mail mit dem AWS SDK for Java \(p. 38\)](#)
- [Senden einer E-Mail mit dem AWS SDK for PHP \(p. 41\)](#)
- [Senden einer E-Mail mit dem AWS SDK for Ruby \(p. 44\)](#)
- [Senden einer E-Mail mit dem AWS SDK for Python \(Boto\) \(p. 46\)](#)

Senden einer E-Mail mit dem AWS SDK for .NET

Im folgenden Verfahren wird beschrieben, wie Sie mit dem eine E-Mail über Amazon SES senden [Visual Studio](#) und die AWS SDK for .NET.

Diese Lösung wurde mit folgenden Komponenten getestet:

- Microsoft Visual Studio Community 2017, Version 15.4.0.
- Microsoft .NET Framework, Version 4.6.1.
- AWSSDK.Core-Paket (Version 3.3.19), installiert mittels NuGet.
- AWSSDK.SimpleEmail-Paket (Version 3.3.6.1), installiert mittels NuGet.

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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#).

Prerequisites

Führen Sie vor Beginn die folgenden Schritte durch:

- Amazon Simple Email Service— Bevor Sie E-Mails mit Amazon 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. Dies lässt sich am einfachsten mit der Amazon SES Konsole durchführen. Weitere Informationen finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
- Abrufen Ihrer AWS Anmeldein— Sie benötigen eine AWS Zugriffsschlüssel-ID und einen geheimen AWS-Zugriffsschlüssel, um über ein SDK auf Amazon SES zuzugreifen. Sie erhalten Ihre Anmeldeinformationen über die Seite [Security Credentials \(Sicherheitsanmeldeinformationen\)](#) der AWS

Management Console. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen](#) (p. 18).

- Installieren von Visual Studio—Visual Studio ist verfügbar unter <https://www.visualstudio.com/>.
- Erstellen einer freigegebenen Anmeldeinformationsdatei— Damit der Beispiel-Code in diesem Abschnitt ordnungsgemäß funktioniert, müssen Sie eine gemeinsame Anmeldeinformationsdatei erstellen. Weitere Informationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34) .

Procedure

Im folgenden Verfahren wird beschrieben, wie Sie mit dem Amazon SES über sendenAWS SDK for .NET.

So senden Sie eine E-Mail mit dem AWS SDK for .NET

1. Führen Sie die folgenden Schritte aus, um ein neues Projekt zu erstellen:
 - a. Starten Sie Visual Studio.
 - b. Wählen Sie im Menü Datei Neu, Projekt aus.
 - c. Erweitern Sie im linken Bereich des Fensters Neues Projekt die Einträge 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. Integrieren Sie mithilfe von NuGet die Amazon SES Pakete in Ihre Lösung, indem Sie die folgenden Schritte ausführen:
 - a. Klicken Sie im Bereich Solution Explorer mit der rechten Maustaste auf Ihr Projekt, und wählen Sie dann Manage NuGet PackagesHerr aus.
 - b. Klicken Sie auf derNuGet AmazonSESSampleWählen Sie auf der RegisterkarteDurchsuchen.
 - c. Geben Sie in das Suchfeld **AWSSDK.SimpleEmail** ein.
 - d. Wählen Sie das Paket AWSSDK.SimpleEmail und anschließend Install aus.
 - e. Klicken Sie im Fenster 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 for .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 for .NET.";

// The HTML body of the email.
static readonly string htmlBody = @"<html>
<head></head>
<body>
  <h1>Amazon SES Test (AWS SDK for .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 for .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.WriteLine("Press any key to continue...");  
        Console.ReadKey();  
    }  
}
```

4. Führen Sie im Code-Editor die folgenden Schritte aus:

- Ersetzen `sender@example.com` mit dem „Von:“ E-Mail-Adresse. Diese Adresse muss verifiziert werden. Weitere Informationen finden Sie unter [the section called “Verifizieren von Identitäten” \(p. 52\)](#).
- Ersetzen `recipient@example.com` mit dem „To:“ Adresse. Wenn sich Ihr Konto noch in der Sandbox befindet, muss auch diese Adresse verifiziert werden.
- Ersetzen Sie `ConfigSet` durch den Namen des Konfigurationssatzes, der beim Senden dieser E-Mail verwendet wird.
- Ersetzen `USWest2` mit dem Namen des Endpunkts der AWS Region, die Sie zum Senden der E-Mail mit Amazon SES verwenden. Eine Liste der Regionen, in denen Amazon SES erhältlich ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen 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 Erstellen Projektmappe erstellen aus.
 - b. Klicken Sie im Menü Debuggen auf 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.

Senden einer E-Mail mit dem AWS SDK for Java

Das folgende Verfahren zeigt, wie Sie [Eclipse IDE für Java EE Entwickler](#) und [AWS Toolkit for Eclipse](#) Wenn Sie ein AWS S-SDK-Projekt erstellen und den Java-Code ändern, um eine E-Mail über Amazon SES zu senden.

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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#).

Prerequisites

Führen Sie vor Beginn die folgenden Schritte durch:

- Amazon Simple Email Service— Bevor Sie E-Mails mit Amazon 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. Dies lässt sich am einfachsten mit der Amazon SES Konsole durchführen. Weitere Informationen finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
- Abrufen Ihrer AWS Anmeldein— Sie benötigen eine AWS Zugriffsschlüssel-ID und einen geheimen AWS-Zugriffsschlüssel, um über ein SDK auf Amazon SES zuzugreifen. Sie erhalten Ihre Anmeldeinformationen über die Seite [Security Credentials \(Sicherheitsanmeldeinformationen\)](#) in der

AWS Management Console. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen](#) (p. 18).

- Installieren von Eclipse—Eclipse ist verfügbar unter <https://www.eclipse.org/downloads>. 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 den AWS Toolkit for Eclipse – Anweisungen zum Hinzufügen des 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.
- Erstellen einer freigegebenen Anmeldeinformationsdatei— Damit der Beispiel-Code in diesem Abschnitt ordnungsgemäß funktioniert, müssen Sie eine gemeinsame Anmeldeinformationsdatei erstellen. Weitere Informationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34) .

Procedure

Im folgenden Verfahren wird beschrieben, wie Sie mit dem Amazon SES über `sendEmail` AWS SDK for Java.

So senden Sie eine E-Mail mit dem AWS SDK for 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 die Option New und wählen Sie dann Other aus. Erweitern Sie im Fenster New den Ordner AWS und wählen Sie dann AWS Java Project aus.
 - c. Führen Sie im Dialogfeld New AWS Java Project die folgenden Schritte aus:
 - i. Geben Sie im Feld Project name einen Namen für das Projekt ein.
 - ii. `UNDERAWS SDK for JavaBeispiele`Wählen Sie bei `JavaMail Service — Beispiel für Amazon Simple Email Service`.
 - iii. Klicken Sie auf Finish.
2. Erweitern Sie im Bereich Package 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 for Java)";

// The HTML body for the email.
static final String HTMLBODY = "<h1>Amazon SES test (AWS SDK for 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 for 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 [Überprüfen von Identitäten in Amazon SES \(p. 52\)](#).
- `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 [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

- (Optional)**us-west-2**— Wenn Sie Amazon SES in einer anderen Region als US West (Oregon) verwenden möchten, ersetzen Sie dies durch die entsprechende Region. Eine Liste der Regionen, in denen Amazon SES erhältlich ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen AWS-Referenz.
6. Speichern `AmazonSESSample.java`.
 7. Wählen Sie Project (Projekt) und dann Build Project (Build-Projekt) 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 und dann erneut Run 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.

Senden einer E-Mail mit dem AWS SDK for PHP

In diesem Thema erfahren Sie, wie Sie die [AWS SDK for PHP](#), um eine E-Mail über Amazon SES zu senden.

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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#).

Prerequisites

Führen Sie vor Beginn die folgenden Schritte durch:

- Amazon Simple Email Service— Bevor Sie E-Mails mit Amazon 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. Dies lässt sich am einfachsten mit der Amazon SES Konsole durchführen. Weitere Informationen finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
- Abrufen Ihrer AWS Anmeldein— Sie benötigen eine AWS Zugriffsschlüssel-ID und einen geheimen AWS-Zugriffsschlüssel, um über ein SDK auf Amazon SES zuzugreifen. Sie erhalten Ihre Anmeldeinformationen über die Seite [Security Credentials \(Sicherheitsanmeldeinformationen\)](#) der AWS Management Console. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#).
- 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.
- Installieren der AWS SDK for PHP-Version 3 – Anweisungen zum Herunterladen und Installieren finden Sie in der [AWS SDK for PHP-Dokumentation](#). Der Code in diesem Tutorial wurde unter Verwendung der Version 3.64.13 des SDKs getestet.
- Erstellen einer freigegebenen Anmeldeinformationsdatei— Damit der Beispiel-Code in diesem Abschnitt ordnungsgemäß funktioniert, müssen Sie eine gemeinsame Anmeldeinformationsdatei erstellen. Weitere Informationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei \(p. 34\)](#).

Procedure

Im folgenden Verfahren wird beschrieben, wie Sie mit dem Amazon SES über sendenAWS SDK for PHP.

So senden Sie mit dem dem eine E-Mail über Amazon SESAWS SDK for 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 for 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 for 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** – Ersetzen Sie diese Zeichenfolge durch den Pfad, der erforderlich ist, um das AWS SDK for PHP in das Programm einzuschließen. Weitere Informationen finden Sie in der [AWS SDK for PHP-Dokumentation](#).
- **sender@example.com**— Ersetzen Sie dies durch eine E-Mail-Adresse, die für Amazon SES verifiziert wurde. Weitere Informationen finden Sie unter [Verifizieren von Identitäten \(p. 52\)](#) . Bei 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 die Adressen Ihrer Empfänger. Wenn sich Ihr Konto noch in der Sandbox befindet, muss auch die Empfängeradresse verifiziert werden. Weitere Informationen finden Sie unter [Verlassen der Amazon SES -Sandbox \(p. 79\)](#) . 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, ersetzen Sie diesen Wert durch den Namen des Konfigurationssatzes. Weitere Informationen zu Konfigurationssätzen finden Sie unter [Verwenden von Amazon SES Konfigurationssätzen \(p. 271\)](#).
- (Optional)**us-west-2**— Wenn Sie Amazon SES in einer anderen Region als US West (Oregon) verwenden möchten, ersetzen Sie dies durch die entsprechende Region. Eine Liste der Regionen, in denen Amazon SES erhältlich ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen 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 Sie einen „cURL Fehler 60 stoßen: Wenn Sie das Programm ausführen, laden Sie das neueste CA-Bundle herunter, wie im [AWS SDK for PHP-Dokumentation](#). 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.

Senden einer E-Mail mit dem AWS SDK for Ruby

In diesem Thema erfahren Sie, wie Sie die [AWS SDK for Ruby](#), um eine E-Mail über Amazon SES zu senden.

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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#).

Prerequisites

Führen Sie vor Beginn die folgenden Schritte durch:

- Amazon Simple Email Service— Bevor Sie E-Mails mit Amazon 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. Dies lässt sich am einfachsten mit der Amazon SES Konsole durchführen. Weitere Informationen finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
- Abrufen Ihrer AWS Anmeldein— Sie benötigen eine AWS Zugriffsschlüssel-ID und einen geheimen AWS-Zugriffsschlüssel, um über ein SDK auf Amazon SES zuzugreifen. Sie erhalten Ihre Anmeldeinformationen über die Seite [Security Credentials \(Sicherheitsanmeldeinformationen\)](#) der AWS Management Console. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#).
- Installieren von Ruby—Ruby ist verfügbar unter <https://www.ruby-lang.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 des AWS SDK for RubyAnweisungen zum Herunterladen und Installieren finden Sie unter [Installieren des AWS SDK for Ruby](#) im AWS SDK for Ruby Entwicklerhandbuch. Der Beispiel-Code in diesem Tutorial wurde mit Version 2.9.36 des AWS SDK for Ruby getestet.
- Erstellen einer freigegebenen Anmeldeinformationsdatei— Damit der Beispiel-Code in diesem Abschnitt ordnungsgemäß funktioniert, müssen Sie eine gemeinsame Anmeldeinformationsdatei erstellen. Weitere Informationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei \(p. 34\)](#).

Procedure

Im folgenden Verfahren wird beschrieben, wie Sie mit dem Amazon SES über senden AWS SDK for Ruby.

So senden Sie mit dem dem eine E-Mail über Amazon SES AWS SDK for 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 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 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 [Verifizieren von Identitäten \(p. 52\)](#) . Bei 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 [Verlassen der Amazon SES -Sandbox \(p. 79\)](#) . Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
 - (Optional) **us-west-2**— Wenn Sie Amazon SES in einer anderen Region als US West (Oregon) verwenden möchten, ersetzen Sie dies durch die entsprechende Region. Eine Liste der Regionen, in denen Amazon SES erhältlich ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen 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.

Senden einer E-Mail mit dem AWS SDK for Python (Boto)

In diesem Thema erfahren Sie, wie Sie die [AWS SDK for Python \(Boto\)](#), um eine E-Mail über Amazon SES zu senden.

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 Ihrer Unzustellbarkeits- und Beschwerderate. Weitere Informationen finden Sie unter [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#) .

Prerequisites

Führen Sie vor Beginn die folgenden Schritte durch:

- Amazon Simple Email Service— Bevor Sie E-Mails mit Amazon 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. Dies lässt sich am einfachsten mit der Amazon SES Konsole durchführen. Weitere Informationen finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#) .
- Abrufen Ihrer AWS Anmelde-ID— Sie benötigen eine AWS Zugriffsschlüssel-ID und einen geheimen AWS-Zugriffsschlüssel, um über ein SDK auf Amazon SES zuzugreifen. Sie erhalten Ihre

Anmeldeinformationen über die Seite [Security Credentials \(Sicherheitsanmeldeinformationen\)](#) der AWS Management Console. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen](#) (p. 18).

- Installieren von Python—Python ist verfügbar unter <https://www.python.org/downloads/>. 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 des AWS SDK for Python (Boto) – Anweisungen zum Herunterladen und Installieren finden Sie in der [AWS SDK for Python \(Boto\)-Dokumentation](#). Der Beispiel-Code in diesem Tutorial wurde mit Version 1.4.4 des SDK für Python getestet.
- Erstellen einer freigegebenen Anmeldeinformationsdatei— Damit der Beispiel-Code in diesem Abschnitt ordnungsgemäß funktioniert, müssen Sie eine gemeinsame Anmeldeinformationsdatei erstellen. Weitere Informationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34) .

Procedure

Im folgenden Verfahren wird beschrieben, wie Sie mit dem SDK für Python eine E-Mail über Amazon SES senden.

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 for 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 for 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 [Verifizieren von Identitäten \(p. 52\)](#) . Bei 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 [Verlassen der Amazon SES -Sandbox \(p. 79\)](#) . Stellen Sie sicher, dass die von Ihnen eingegebene Adresse exakt mit der verifizierten Adresse übereinstimmt.
- (Optional)**us-west-2**— Wenn Sie Amazon SES in einer anderen Region als US West (Oregon) verwenden möchten, ersetzen Sie dies durch die entsprechende Region. Eine Liste der Regionen, in denen Amazon SES erhältlich ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen 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.

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

Dieses Thema bietet eine Übersicht über die Schritte, die Sie ausführen müssen, wenn Sie Ihre E-Mail-Lösung von einer On-Premise gehosteten Lösung oder von einer auf einer Amazon EC2-Instance gehosteten Lösung zu Amazon SES verschieben möchten.

Themen in diesem Abschnitt:

- [Überprüfen Ihrer Domäne](#) (p. 49)
- [Anfordern von Produktionszugriff](#). (p. 49)
- [Konfigurieren von Domänenauthentifizierungssystemen](#) (p. 49)
- [Erstellen Ihrer SMTP-Anmeldeinformationen](#) (p. 50)
- [Herstellen einer Verbindung mit einem SMTP-Endpunkt](#) (p. 50)
- [Nächste Schritte](#) (p. 50)

Überprüfen Ihrer Domäne

Bevor Sie Amazon SES zum Senden von E-Mails verwenden können, müssen Sie die Identitäten überprüfen, von denen Sie E-Mails senden möchten. In Amazon SES kann eine Identität eine E-Mail-Adresse oder eine ganze Domäne sein. Wenn Sie eine Domäne verifizieren, können Sie Amazon SES zum Senden von E-Mails von einer beliebigen Adresse in dieser Domäne aus verwenden. Weitere Informationen zum Verifizieren von Domänen finden Sie unter [Überprüfen von Domänen in Amazon SES](#) (p. 65).

Anfordern von Produktionszugriff.

Wenn Sie Amazon SES zum ersten 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 [Verlassen der Amazon SES - Sandbox](#) (p. 79).

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](#) (p. 141). Weitere Informationen zur Einrichtung von DKIM finden Sie unter [Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES](#) (p. 142).

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 AWS S-Anmeldeinformationen identisch. Diese Anmeldeinformationen sind auch in jeder AWS Region eindeutig. Weitere Informationen zum Abrufen Ihrer SMTP-Anmeldeinformationen finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen](#) (p. 95).

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 einem Amazon SES SMTP-Endpunkt](#) (p. 100). 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](#) (p. 271) .
- Wenn Sie E-Mail-Nachrichten über Amazon SES senden, ist es wichtig, die Unzustellbarkeitsereignisse und Beschwerden für Ihr Konto zu überwachen. Amazon SES enthält ein Zuverlässigkeitsdashboard, mit dem Sie die Unzustellbarkeitsereignisse und Beschwerden für Ihr Konto verfolgen können. Weitere Informationen finden Sie unter [Verwenden des Reputation Dashboards zum Nachverfolgen von Unzustellbarkeits- und Beschwerdequoten](#) (p. 400) . Sie können auch CloudWatch-Alarme erstellen, die Sie benachrichtigen, wenn diese Werte zu hoch werden. Weitere Hinweise zum Erstellen von CloudWatch-Alarmen finden Sie unter [Erstellen von Zuverlässigkeitsüberwachungsalarmen mit CloudWatch](#) (p. 415).
- 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](#) (p. 188) .

Einrichten von E-Mail mit Amazon SES

Zum Einrichten von E-Mail mit Amazon Simple Email Service (Amazon SES) gehen Sie wie folgt vor:

- Bevor Sie auf Amazon SES oder andere AWS -Services zugreifen können, müssen Sie ein AWS-Konto einrichten. Weitere Informationen finden Sie unter [Registrieren bei AWS](#) (p. 51) .
- Bevor Sie E-Mails über Amazon SES senden, müssen Sie sicherstellen, dass Sie Besitzer der „From“-Adresse sind. Verifizieren Sie auch die „To“-Adresse, wenn sich Ihr Konto noch in der Amazon SES Sandbox befindet. Sie können E-Mail-Adressen oder ganze Domänen verifizieren. Weitere Informationen finden Sie unter [Überprüfen von Identitäten in Amazon SES](#) (p. 52) .

Die folgenden Aufgaben sind optional und hängen davon ab, wofür Sie die Anwendung nutzen möchten:

- Wenn Sie über die Amazon SES -API auf Amazon SES zugreifen möchten, sei es direkt über die Abfrage (HTTPS) -Schnittstelle oder indirekt über eine [AWS SDK](#), die [AWS Command Line Interface](#) oder die [AWS Tools for Windows PowerShell](#) Sie müssen Ihre AWS Zugriffsschlüssel abrufen. Weitere Informationen finden Sie unter [Abrufen von AWS-Zugriffsschlüsseln \(p. 71\)](#) .
- Wenn Sie die Amazon SES -API aufrufen möchten, ohne sich mit den einfachen Details der Abfrageschnittstelle auseinanderzusetzen, können Sie ein AWS SDK verwenden. Weitere Informationen finden Sie unter [Herunterladen eines AWS SDKs \(p. 72\)](#) .
- Wenn Sie auf Amazon SES über die SMTP-Schnittstelle zugreifen möchten, benötigen Sie einen SMTP-Benutzernamen und ein SMTP-Passwort. Ihre SMTP-Anmeldeinformationen sind nicht mit den AWS-Anmeldeinformationen identisch. Weitere Informationen finden Sie unter [Einrichten Ihrer SMTP-Anmeldeinformationen für Amazon SES \(p. 79\)](#) .
- Wenn Sie sich das erste Mal bei Amazon SES anmelden, befindet sich Ihr Konto in der Amazon SES Sandbox. In der Sandbox können Sie E-Mails mit denselben Sendemethoden verschicken wie andere Amazon SES S-Benutzer. Die Anzahl der E-Mails, die Sie versenden dürfen, darf allerdings innerhalb von 24 Stunden 200 nicht überschreiten. Dabei wird maximal eine E-Mail pro Sekunde verschickt. Die Zustellung erfolgt zudem nur an von Ihnen nachgewiesene Adressen. Zur Erhöhung Ihrer Sendekontingente und zum Senden von E-Mails an nicht verifizierte E-Mail-Adressen lesen Sie [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).
- Wenn Sie möchten, dass Ihre E-Mails eine Domain-based Message Authentication, Reporting and Conformance (DMARC)-Authentifizierung basierend auf einem Sender Policy Framework (SPF) durchlaufen, konfigurieren Sie Ihre Identität so, dass E-Mails von einer benutzerdefinierten MAIL FROM-Domäne verschickt werden, wie unter [Einrichten einer benutzerdefinierten MAIL FROM-Domäne \(p. 72\)](#) beschrieben.

Registrieren bei AWS

Sie müssen ein AWS Konto einrichten, ehe Sie auf Amazon SES oder andere AWS-Services zugreifen können.

So erstellen Sie ein Amazon-Konto

1. Navigieren Sie in einem Webbrowser zu <https://aws.amazon.com/ses>.
2. Klicken Sie auf Erstellen eines AWS-Kontos.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Nächste Schritte

Nachdem Sie Ihr AWS Konto erstellt haben, können Sie mit der Einrichtung von Amazon SES beginnen.

- Um E-Mails mit Amazon SES zu senden, müssen Sie zuerst [Überprüfen einer Identität \(p. 52\)](#). Eine Identität ist eine E-Mail-Adresse oder Domäne, von der Ihre E-Mail gesendet wird.
- Um mit Amazon SES zu interagieren, müssen Sie [Abrufen der IAM-Anmeldeinformationen \(p. 71\)](#) für Ihr -Konto.
- Wenn Sie Amazon SES zum ersten Mal verwenden, befindet sich Ihr Konto in der Amazon SES Sandbox. Über die Sandbox haben Sie vollen Zugriff auf die Amazon SES -API und die SMTP-Schnittstelle. Es gelten jedoch folgende Einschränkungen:
 - Sie können E-Mails nur an die [Amazon SES Postfachsimulator \(p. 198\)](#), und [Verifizierte E-Mail-Identitäten \(p. 52\)](#).
 - Sie können innerhalb von 24 Stunden nur maximal 200 E-Mails versenden.
 - Pro Sekunden kann nur eine Nachricht verschickt werden.

Weitere Informationen zum Verlassen der Sandbox finden Sie unter [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

Überprüfen von Identitäten in Amazon SES

In Amazon SES wird eine Identität eine E-Mail-Adresse oder Domäne, mit der Sie E-Mails senden. 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. Ist Ihr Konto noch in der Amazon SES -Sandbox, müssen Sie alle E-Mail-Adressen verifizieren, an die Sie Nachrichten schicken, mit Ausnahme derer, die vom [Amazon SES Postfachsimulator](#) (p. 198).

Sie können eine Identität mithilfe der Amazon SES Konsole oder der Amazon SES-API verifizieren.

Amazon Verifizieren von E-Mail-Adressen in Amazon SES

Amazon SES erfordert, dass Sie Ihre Identitäten (Domänen und E-Mail-Adressen, von denen Sie E-Mails senden), um zu bestätigen, dass es sich wirklich um eigenen E-Mail-Adressen handelt, und um eine unbefugten Nutzung zu verhindern. Dieser Abschnitt enthält Informationen zur Verifizierung der Identitäten von E-Mail-Adressen. Weitere Informationen zum Verifizieren von Domänen-Identitäten finden Sie unter [the section called "Verifizieren von Domänen"](#) (p. 65).

Beachten Sie die folgenden Faktoren, wenn Sie E-Mail-Adressen für die Verwendung mit Amazon SES verifizieren:

- Sie müssen jede Identität verifizieren, die Sie als Adresse unter „From“, „Source“, „Sender“ oder „Return-Path“ angeben. Sie können bereits verifizierten E-Mail-Adressen jedoch eine Kennung hinzuzufügen, ohne zusätzliche Verifizierungsschritte durchzuführen (siehe Informationen weiter unten in dieser Liste).
- 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.
- Wenn Sie sowohl eine E-Mail-Adresse als auch die Domäne verifizieren, der die Adresse angehört, dann setzen die Einstellungen für die E-Mail-Adresse die Einstellungen der Domäne außer Kraft. Beispiel: Wenn DomainKeys Identified Mail (DKIM) für die Domäne `example.com` aktiviert ist, jedoch nicht für `sender@example.com`, dann sind die von `sender@example.com` gesendeten E-Mails nicht DKIM-signiert.
- Amazon SES verfügt über Endpunkte in mehreren AWS Regionen, und der Verifizierungsstatus der E-Mail-Adresse gilt pro Region. Wenn Sie E-Mails von derselben Identität in mehr als einer Region senden möchten, müssen Sie diese Identität in jeder Region verifizieren. Weitere Informationen über die Verwendung von Amazon SES in mehreren Regionen finden Sie unter [Regionen](#) (p. 494).
- Sie können pro AWS Region bis zu 10.000 Identitäten (E-Mail-Adressen oder Domänen in beliebiger Kombination) verifizieren.
- Sie können verifizierten E-Mail-Adressen Kennzeichen hinzufügen, ohne zusätzliche Verifizierungsschritte durchzuführen. Um einer E-Mail-Adresse ein Kennzeichen hinzuzufügen, 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.
- Sie können die Nachrichten anpassen, die an die zu verifizierenden E-Mail-Adressen gesendet werden. Weitere Informationen finden Sie unter [Verwenden von benutzerdefinierten Vorlagen zur E-Mail-Verifizierung](#) (p. 57).

Verifizieren einer E-Mail-Adresse

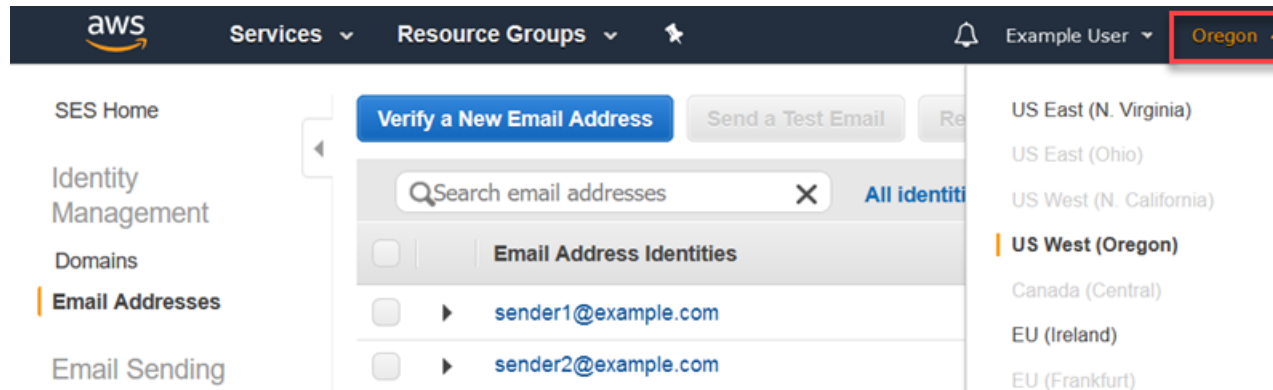
Sie können E-Mail-Adressen mithilfe der Amazon SES Konsole, der [VerifyEmailIdentity](#) Amazon SES API v1-Vorgang oder die [CreateEmailIdentity](#) Amazon SES API v2-Vorgang. Für verbesserte Funktionen empfehlen wir die Verwendung von Amazon SES API v2.

So verifizieren einer E-Mail-Adresse mithilfe der Amazon SES Konsole

Führen Sie das Verfahren in diesem Abschnitt durch, um eine E-Mail-Adresse mithilfe der Amazon SES - Konsole zu verifizieren.

So verifizieren einer E-Mail-Adresse mithilfe der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie in der Konsole mithilfe der Regionsauswahl die AWS Region aus, in der Sie E-Mail-Adresse verifizieren möchten, wie in der folgenden Abbildung dargestellt.



Note

Um eine E-Mail-Adresse für die Verwendung in mehr als einer Region zu verifizieren, wiederholen Sie die Schritte in diesem Abschnitt für jede Region.

3. Wählen Sie im Navigationsbereich unter Identity Management die Option Email Addresses aus.
4. Wählen Sie Verify a New Email Address aus.
5. Geben Sie im Dialogfeld Verify a New Email Address Ihre E-Mail-Adresse in das Feld Email Address ein und wählen Sie Verify This Email Address.
6. 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 RegionRegionName„wobeiRegionNameKlicken Sie auf den Namen der AWS Region, die Sie in Schritt 2 ausgewählt haben.

Klicken Sie auf den Link in der Nachricht.

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.

7. Klicken Sie in der Amazon SES Konsole unterIdentitätsmanagement, wählen SieE-Mail-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“.

Verifizieren einer E-Mail-Adresse mithilfe der Amazon SES API

Sie können die Berechtigung[VerifyEmailIdentity](#)Amazon SES API v1-Vorgang oder die[CreateEmailIdentity](#)Vorgang Amazon SES API v2, um eine neue E-Mail-Identität zu erstellen. Eine einfache Möglichkeit, diese Operationen für individuelle Identitäten aufzurufen, besteht darin, den AWS CLI zu verwenden.

Informationen zum Festlegen eines Standardkonfigurationssatzes beim Überprüfen einer E-Mail-Identität finden Sie unter [Verwalten von Amazon SES Standardkonfigurationssätzen](#) (p. 274).

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](#).

So überprüfen Sie eine E-Mail-Adresse mit der AWS CLI:

1. Geben Sie in der Befehlszeile den folgenden Befehl ein, um die [VerifyEmailIdentity](#) Amazon SES API v1-Vorgang:

```
aws ses verify-email-identity --email-address sender@example.com
```

Ersetzen Sie im voranstehenden Befehl *sender@example.com* durch die E-Mail-Adresse, die Sie verifizieren möchten.

Geben Sie in der Befehlszeile den folgenden Befehl ein, um die [CreateEmailIdentity](#) Amazon SES API v2-Vorgang:

```
aws sesv2 create-email-identity --email-identity sender@example.com
```

Ersetzen Sie im voranstehenden Befehl *sender@example.com* durch die E-Mail-Adresse, die Sie verifizieren möchten.

Bei erfolgreicher Ausführung wird der Befehl ohne Ausgabe beendet.

2. 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 *RegionName* ist der Name der AWS Region, in der Sie versucht haben, die E-Mail-Adresse zu überprüfen.

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.

3. Klicken Sie in der Amazon SES Konsole unter [Identitätsmanagement](#), wählen Sie [E-Mail-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“.

Für einen Skript, mit dem Sie mehrere E-Mail-Identitäten in einer einzelnen Operation verifizieren können, informieren Sie sich unter [the section called “Verifizieren mehrerer E-Mail-Adressen”](#) (p. 487).

Fehlerbehebung bei der Verifizierung der E-Mail-Adresse

Wenn Sie bei dem Versuch, eine E-Mail-Adresse zu verifizieren, keine Verifizierungs-E-Mail von AWS erhalten, führen Sie die folgenden Schritte zur Fehlerbehebung durch:

- Überprüfen Sie den Junk-Ordner in Ihrem E-Mail-Client.
- Vergewissern Sie sich, dass Ihr E-Mail-Client keine Regeln anwendet, die bestimmte Nachrichten automatisch in einen anderen Ordner als Ihren Posteingang verschieben.

- Fügen Sie in Ihrem E-Mail-Client zu Ihrem Adressbuch oder zur Liste sicherer Absender `no-reply-aws@amazon.com` hinzu. Sie können den Systemadministrator auch bitten, eingehende E-Mails von `no-reply-aws@amazon.com` auf die Liste erlaubter Absender (Whitelist) zu setzen.
- Senden Sie bei einer E-Mail-Adresse, die einen anderen E-Mail-Dienstanbieter verwendet (z. B. eine persönliche E-Mail-Adresse), eine Nachricht an die Adresse, die Sie verifizieren möchten. Stellen Sie sicher, dass die Adresse, die Sie verifizieren möchten, die Nachricht empfängt. Dieser Schritt ist besonders wichtig, wenn Sie vor Kurzem eine eigene Domäne eingerichtet haben. Es kann vorkommen, dass neue Domänen für den Empfang eingehender E-Mails nicht korrekt konfiguriert sind.

Alternativ können Sie eine E-Mail-Adresse, die bekanntlich E-Mails empfangen kann, wie z. B. eine persönliche E-Mail-Adresse, verifizieren. Wenn Sie die Verifizierungs-E-Mail an Ihrer persönlichen Adresse empfangen können, kann dies auf ein Problem auf der anderen Domäne hinweisen.

Wenn diese Test zeigen, dass an der zu verifizierenden Adresse keine E-Mails empfangen werden, wenden Sie sich an Ihren Systemadministrator oder E-Mail-Dienstanbieter, um weitere Unterstützung zu erhalten.

Auflisten von E-Mail-Identitäten in Amazon SES

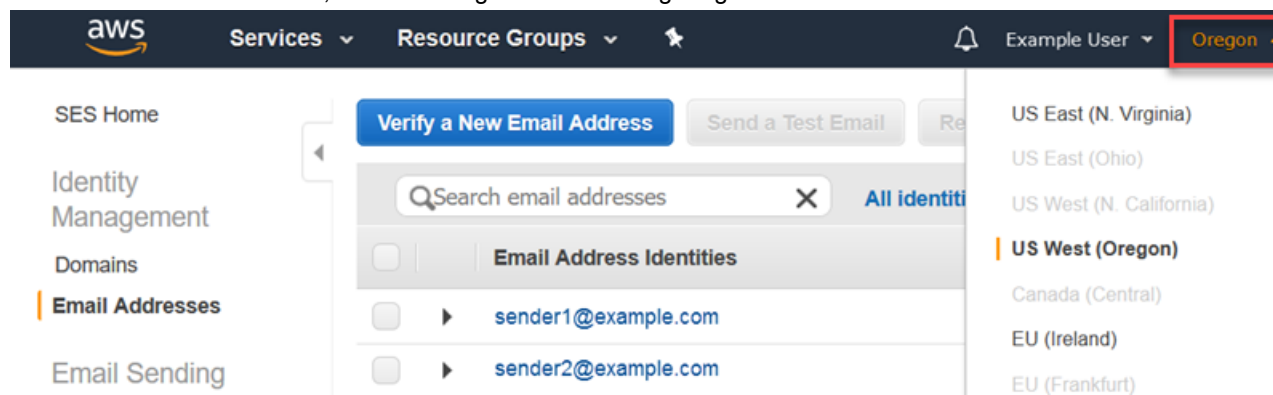
Sie können eine Liste von E-Mail-Identitäten mithilfe der Amazon SES Konsole oder der [ListIdentitiesAPI](#)-Operation

Anzeigen einer Liste von E-Mail-Identitäten in Amazon SES

Sie können mit der Amazon SES Konsole und API eine Liste der E-Mail-Adressen anzeigen, die verifiziert wurden oder bei denen eine Verifizierung aussteht, sowie solche, die den Verifizierungsvorgang nicht bestanden haben.

So zeigen eine Liste der verifizierten E-Mail-Adressen an

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie in der Konsole mithilfe der Regionsauswahl die AWS Region aus, in der Sie E-Mail-Identitäten auflisten möchten, wie in der folgenden Abbildung dargestellt.



Note

Diese Verfahren zeigen nur eine Liste der E-Mail-Adressen für die ausgewählte AWS Region an.

3. Wählen Sie im Navigationsbereich unter Identity Management die Option Email Addresses aus.

Die Seite der E-Mail-Adressen zeigt eine Liste von E-Mail-Adressen an, die verifiziert wurden, bei denen eine Verifizierung aussteht oder die den Verifizierungsvorgang nicht bestanden haben. Klicken Sie auf eine E-Mail-Adresse, um weitere Informationen darüber anzuzeigen.

Anzeigen einer Liste von E-Mail-Identitäten mithilfe der Amazon SES -API

Verwenden Sie die API-Operation [ListIdentities](#), um eine Liste aller E-Mail-Identitäten, unabhängig von deren Status, anzuzeigen. Sie können auch die Operation [GetIdentityVerificationAttributes](#) verwenden, um den Verifizierungsstatus einer bestimmten Identität zu finden.

Um eine Liste der Identitäten mithilfe der AWS CLI anzuzeigen, geben Sie den folgenden Befehl in die Befehlszeile ein: `aws ses list-identities`

Wenn Sie die `ListIdentities` wird eine Liste aller Identitäten in Ihrem Amazon SES -Konto, unabhängig von deren Verifizierungsstatus, zurückgegeben. Mit der Operation `GetIdentityVerificationAttributes` können Sie den Verifizierungsstatus für eine oder mehrere Identitäten anzeigen. Um den Verifizierungsstatus einer Identität mithilfe der AWS CLI zu bestimmen, geben Sie den folgenden Befehl in die Befehlszeile ein: `aws ses get-identity-verification-attributes --identities "sender@example.com"`

Ersetzen Sie `sender@example.com` im voranstehenden Befehl durch die Identität, deren Verifizierungsstatus Sie suchen möchten. Außerdem können Sie mit diesem Befehl den Verifizierungsstatus mehrerer Identitäten in einem einzelnen API-Aufruf suchen. Wenn Sie beispielsweise nach dem Status der Domäne `example.com` und der E-Mail-Adresse `sender@example.co.uk` suchen, möchten, geben Sie den folgenden Befehl ein: `aws ses get-identity-verification-attributes --identities "example.com" "sender@example.co.uk"`

Amazon Löschen einer E-Mail-Identität in Amazon SES

Wenn Sie eine verifizierte E-Mail-Adresse nicht mehr benötigen, können Sie sie mithilfe der Amazon SES -Konsole oder der [DeleteIdentity](#) API-Operation

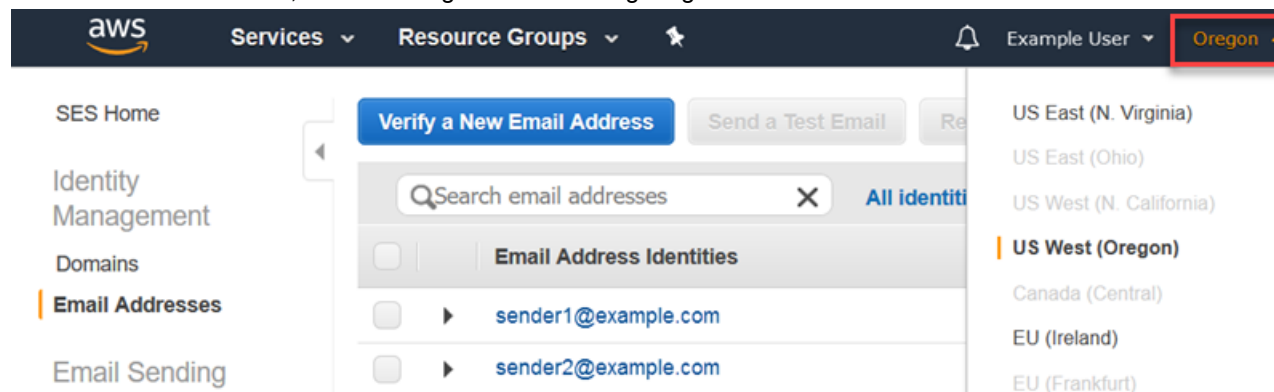
Warning

Diese Aktion kann nicht mehr rückgängig gemacht werden. Sie können den Verifizierungsvorgang für eine zuvor gelöschte Identität jedoch wiederholen.

Amazon Löschen einer E-Mail-Identität in Amazon SES

So entfernen Sie verifizierte E-Mail-Adressen

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie in der Konsole mithilfe der Regionsauswahl die AWS Region aus, in der Sie eine E-Mail-Identität löschen möchten, wie in der folgenden Abbildung dargestellt.



Note

Diese Verfahren löschen nur die E-Mail-Adresse in der ausgewählten AWS Region. Um eine E-Mail-Adresse zu löschen, die in mehr als einer Region verifiziert wurde, wiederholen Sie die Schritte in diesem Abschnitt für jede Region.

3. Wählen Sie jede E-Mail-Adresse aus, die Sie löschen möchten, und klicken Sie dann auf Remove.

Löschen einer E-Mail-Identität mithilfe der Amazon SES API

Mit der API-Operation `DeleteIdentity` können Sie E-Mail-Adresse und Domänenidentitäten löschen.

Um eine Identität mithilfe der AWS CLI zu löschen, geben Sie den folgenden Befehl in die Befehlszeile ein:
`aws ses delete-identity --identity "sender@example.com"`

Ersetzen Sie im voranstehenden Befehl `sender@example.com` durch die Identität, die Sie löschen möchten.

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=AKIAOKE4EXAMPLE&Context=10987654321&Identity.IdentityName=recipient%40example.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=TJDufFhYK1fSHCSBq4qjodBQq%2FnyZgZqZ%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 [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

Themen in diesem Abschnitt:

- [Erstellen einer benutzerdefinierten Vorlage zur E-Mail-Verifizierung \(p. 58\)](#)
- [Bearbeiten einer benutzerdefinierten Vorlage zur E-Mail-Verifizierung \(p. 59\)](#)
- [Senden von Verifizierungs-E-Mails mit benutzerdefinierten Vorlagen \(p. 59\)](#)
- [Benutzerdefinierte Verifizierungs-E-Mail – Häufig gestellte Fragen \(p. 60\)](#)

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	Beschreibung
<code>TemplateName</code>	Der Name der Vorlage. Der angegebene Name muss eindeutig sein.
<code>FromEmailAddress</code>	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. Note Das <code>FromEmailAddress</code> -Attribut unterstützt keine Anzeigenamen (auch bekannt als "friendly from"-Namen).
<code>TemplateSubject</code>	Die Betreffzeile der Verifizierungs-E-Mail.
<code>TemplateContent</code>	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 (p. 60) .
<code>SuccessRedirectionURL</code>	Die URL, die Benutzern gesendet wird, wenn deren E-Mail-Adressen erfolgreich überprüft werden.
<code>FailureRedirectionURL</code>	Die URL, die Benutzern gesendet wird, wenn deren E-Mail-Adressen nicht erfolgreich überprüft werden.

Sie können aber auch die AWS SDKs oder die AWS CLI verwenden. So erstellen Sie eine benutzerdefinierte Vorlage zur E-Mail-Verifizierung mit der `CreateCustomVerificationEmailTemplate`. Weitere Informationen zu den AWS -SDKs finden Sie unter [Tools für Amazon Web Services](#). Weitere Informationen zum AWS CLI finden Sie 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 zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

Note

Um das Verfahren in diesem Abschnitt abzuschließen, müssen Sie Version 1.14.6 oder höher der AWS CLI. Um die besten Ergebnisse zu erzielen, führen Sie ein Upgrade auf die neueste Version der AWS CLI. Weitere Informationen zum Aktualisieren der AWS CLI finden Sie unter [Installieren des AWS Command Line Interface](#) im AWS Command Line Interface-Benutzerhandbuch.

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 die `FromEmailAddress`-Parameter überprüft werden muss oder eine Adresse in einer verifizierten Domäne sein muss. Weitere Informationen finden Sie unter [Überprüfen von Identitäten in Amazon SES \(p. 52\)](#).

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 ses 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 ses 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

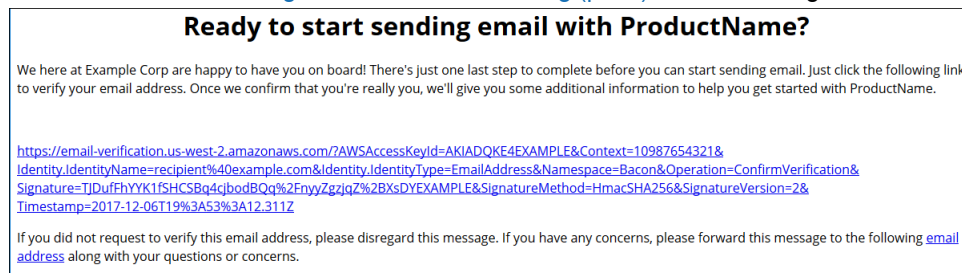
Nachdem Sie mindestens eine benutzerdefinierte Verifizierungs-E-Mail-Vorlage erstellt haben, können Sie sie durch Aufrufen der [SendCustomVerificationEmail](#)-API-Operation an Ihre Kunden senden. Sie können

die Berechtigung `SendCustomVerificationEmail` Verwenden Sie eines der AWS SDKs oder der AWS CLI. Die `SendCustomVerificationEmail`-Operation akzeptiert die folgenden Eingaben:

Attribut	Beschreibung
<code>EmailAddress</code>	Die E-Mail-Adresse, die überprüft wird.
<code>TemplateName</code>	Der Name der benutzerdefinierten Verifizierungs-E-Mail-Vorlage, der an die E-Mail-Adresse gesendet wird, die überprüft wird.
<code>ConfigurationSetName</code>	(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 \(p. 58\)](#) erstellte Vorlage verwendet.



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 `output.txt` gespeichert.

Sie können das Base64-kodierte Abbild einbetten, indem Sie Folgendes in den HTML-Code für die Vorlage einschließen: ``

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
<code>abbr</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>acronym</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>address</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>area</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>b</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>bdo</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>big</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>blockquote</code>	<code>cite</code> , <code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>body</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>br</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>button</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>caption</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>
<code>center</code>	<code>class</code> , <code>id</code> , <code>style</code> , <code>title</code>

HTML-Tag	Zulässige Attribute
cite	class, id, style, title
code	class, id, style, title
col	class, id, span, style, title, width
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	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

HTML-Tag	Zulässige Attribute
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
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

HTML-Tag	Zulässige Attribute
ul	class, id, style, title, type
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 S-Konto kann in jeder AWS Region über bis zu 10.000 verifizierte Identitäten verfügen. Amazon SES-Identitätenschließen 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 Überprüfung dieser E-Mail-Adresse nicht angefordert haben, ignorieren Sie diese Nachricht. Wenn Sie Bedenken haben, leiten Sie diese Nachricht zusammen mit Ihren Fragen oder Anmerkungen an die folgende E-Mail-Adresse weiter.

DieE-Mail-AdresseDer Link in diesem Text bezieht sich auf aws-email-domain-verification@amazon.com, einem Posteingang, der aktiv vom Amazon SES -Team überwacht wird.

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" \(p. 142\)](#).

F12. Warum werden die API-Operationen für die benutzerdefinierte Verifizierungs-E-Mail-Vorlage nicht im SDK oder in der CLI angezeigt?

Wenn Sie die Operationen für die benutzerdefinierte Verifizierungs-E-Mail-Vorlage in einem SDK oder in der AWS CLI nicht verwenden können, haben Sie möglicherweise eine ältere Version des SDK oder der CLI installiert. Die Operationen für die benutzerdefinierte Verifizierungs-E-Mail-Vorlage sind in den folgenden SDKs und CLIs verfügbar:

- AWS Command Line Interface Version 1.14.6 oder höher

- AWS SDK for .NET Version 3.3.205.0 oder höher
- AWS SDK for C++ Version 1.3.20170531.19 oder höher
- AWS SDK for Go Version 1.12.43 oder höher
- AWS SDK for Java Version 1.11.245 oder höher
- AWS SDK for JavaScript Version 2.166.0 oder höher
- AWS SDK for PHP Version 3.45.2 oder höher
- AWS SDK for Python (Boto) Version 1.5.1 oder höher
- `aws-sdk-ses`-Gem in AWS SDK for Ruby, Version 1.5.0 oder höher

F13. Warum erhalte ich `ProductionAccessNotGranted`-Fehler, wenn ich benutzerdefinierte Verifizierungs-E-Mails sende?

Die `ProductionAccessNotGranted` gibt 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 [Verlassen der Amazon SES - Sandbox](#) (p. 79).

Überprüfen von Domänen in Amazon SES

Amazon SES erfordert, dass Sie Ihre E-Mail-Adresse oder Domäne verifizieren, um zu bestätigen, dass diese Ihnen gehört und um zu vermeiden, dass sie von anderen verwendet wird. Wenn Sie eine ganze Domäne verifizieren, verifizieren Sie alle E-Mail-Adressen dieser Domäne, sodass Sie diese nicht einzeln bestätigen müssen. Wenn Sie beispielsweise die Domäne `example.com` verifizieren, können Sie E-Mails von `user1@example.com`, `user2@example.com` oder jedem anderen Benutzer, der der Domäne `example.com` zugeordnet ist, senden.

Sie können die verifizierten Domänen mit der Amazon SES Konsole oder der Amazon SES-API verwalten. Eine vollständige Beschreibung der API-Aktionen für die Domänenverifizierung finden Sie unter [Amazon Simple Email Service API-Referenz](#). In diesem Abschnitt, in dem die Aktionen erläutert werden, die über die Amazon SES Konsole durchgeführt werden, sind folgende Themen enthalten:

- [Verifizieren einer Domäne mit Amazon SES](#) (p. 66)
- [Amazon Auflisten von Domänen-Identitäten in Amazon SES](#) (p. 68)
- [Löschen einer Domänen-Identität in Amazon SES](#) (p. 68)
- [Verifizieren einer Amazon SES S-Domänenverifizierung](#) (p. 69)
- [TXT-Datensätze zur Amazon SES E-Domänenverifizierung](#) (p. 69)

Wichtige Hinweise zur Domänenverifizierung:

- Amazon SES verfügt über Endpunkte in mehreren AWS Regionen. Die Domänenverifizierung erfolgt für jede AWS-Region separat. Sie müssen das gesamte Verfahren der Domänenverifizierung für jede Region einzeln durchführen, in die Sie von einer bestimmten Domäne Nachrichten senden möchten. Wenn Sie dieselbe Domäne in mehreren Regionen verifizieren möchten und Ihr DNS-Anbieter lässt keine TXT-Datensätze desselben Namens zu, finden Sie unter [Häufige Probleme mit der Domänenverifizierung](#) (p. 509) Möglichkeiten, dieses Problem zu umgehen.
- Wenn Sie eine Domäne mit Amazon SES verifizieren, können Sie Nachrichten von jeder beliebigen Subdomäne senden, ohne dass diese explizit verifiziert werden muss. Verifizieren Sie beispielsweise `example.com`, müssen Sie weder `a.example.com` noch `a.b.example.com` separat verifizieren. Wie in [RFC 1034](#) angegeben, kann jeder DNS-Label bis zu 63 Zeichen enthalten; der gesamte Domänenname darf nicht länger als 255 Zeichen sein.
- Wenn Sie eine Domäne bzw. Subdomäne(n) oder E-Mail-Adresse(n) mit gemeinsamer Stammdomäne verifizieren, gelten die verifizierten Identitätseinstellungen (wie Feedback-Benachrichtigungen und Easy DKIM) auf der differenziertesten der von Ihnen verifizierten Ebene. Das heißt:

- 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.
- Bei Domännennamen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie `example.com` verifizieren, können Sie Nachrichten auch von `EXAMPLE.com` senden.
- Sie können pro AWS Region bis zu 10.000 Identitäten (E-Mail-Adressen und Domänen in beliebiger Kombination) verifizieren.

Verifizieren einer Domäne mit Amazon SES

Im folgenden Verfahren wird gezeigt, wie Sie eine Domäne mithilfe der Amazon SES Konsole verifizieren. Wenn Sie stattdessen die Amazon SES API v1 verwenden möchten, finden Sie weitere Informationen unter [Amazon Simple Email Service API-Referenz](#).

Informationen zum Festlegen eines Standardkonfigurationssatzes beim Überprüfen einer E-Mail-Identität finden Sie unter [Verwalten von Amazon SES Standardkonfigurationssätzen \(p. 274\)](#).

Note

Statt das Verfahren in diesem Abschnitt abzuschließen, können Sie auch [Easy DKIM \(p. 143\)](#) aktivieren. Wenn Amazon SES feststellt, dass Sie der DNS-Konfiguration für eine Domäne die DKIM-Datensätze hinzugefügt haben, können Sie auch dann E-Mails aus der Domäne senden, wenn Sie das Verfahren in diesem Abschnitt noch nicht abgeschlossen haben.

So verifizieren Sie eine Domäne

1. Wechseln Sie zu Ihrem [Verifizierte Domänenliste](#) oder führen Sie folgende Schritte aus, um zu dieser zu navigieren:
 - a. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
 - b. Wählen Sie im Navigationsbereich unter Identity Management die Option Domains aus.
2. Wählen Sie **Verify a New Domain** aus.
3. Geben Sie im Dialogfeld **Verify a New Domain** den Domännennamen ein.

Tip

Wenn Ihre Domäne `www.example.com` ist, geben Sie `example.com` als Ihre Domäne ein. Das „www.“ Der Domänenverifizierungsprozess wird nicht erfolgreich sein, wenn Sie ihn einschließen.

4. Wenn Sie eine DKIM-Signatur einrichten möchten, klicken Sie auf die Option **Generate DKIM Settings**. Weitere Informationen zur DKIM-Signatur finden Sie unter [Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES \(p. 142\)](#).
5. Wählen Sie **Verify this Domain** aus.

6. Im Dialogfeld **Verify a New Domain** sehen Sie einen Domänenverifizierungs-Datensatz mit Name, Typ und Wert. (Diese Informationen sind auch verfügbar, wenn Sie nach dem Schließen des Dialogfelds den Domännennamen auswählen.)

Fügen Sie zum Abschließen der Domänenverifizierung einen TXT-Datensatz mit dem angezeigten Namen und dem angezeigten Wert zum DNS-Server der Domäne hinzu. Weitere Informationen zu Amazon SES TXT-Datensätzen und allgemeine Anleitungen zum Hinzufügen eines TXT-Datensatzes zu einem DNS-Server finden Sie unter [TXT-Datensätze zur Amazon SES E-Domänenverifizierung](#) (p. 69). Insbesondere:

- Wenn Ihr DNS-Anbieter Unterstriche im Datensatznamen nicht zulässt, können Sie `_amazonses` im Feld Name weglassen.
- Damit Sie diesen Datensatz in den DNS-Einstellungen Ihrer Domäne leicht finden können, können Sie für Value das Präfix `amazonses:` verwenden.
- Einige DNS-Anbieter hängen den Domännennamen automatisch an die Namen von DNS-Datensätzen an. Zur Vermeidung doppelter Domännennamen können Sie im DNS-Datensatz einen Punkt an das Ende des Domännennamens einfügen. Dadurch wird angegeben, dass der Datensatzname vollständig qualifiziert ist und der DNS-Anbieter keinen weiteren Domännennamen anhängen muss.

Verify a New Domain

The domain **example.com** has been added to the list of Verified Senders with a Status of "pending verification". Further action is needed to complete verification of this domain. See details below.

In order to complete verification of **example.com**, you must create the following records in the DNS settings for the domain, with the following values:

Domain Verification Record Set

Name	Type	Value
<code>_amazonses.example.com</code>	TXT	<code>38BnuGvLZI3OZtQP+RRznLBdvhOqoz5tNqH4sKmB/pl=</code>

If your DNS provider does not allow underscores in record names, you can omit `_amazonses` from the record name. To help you easily identify this record within your domain's DNS settings, you can optionally prefix the record value with `amazonses:`. For more information about Amazon SES TXT records and general guidance on how to add a TXT record to a DNS server, see [Amazon SES Domain Verification TXT Records](#).

[Download Record Set as CSV »](#)

Close

7. Wenn Route 53 den DNS-Service für die Domäne bereitstellt, die Sie verifizieren, und Sie bei der AWS Management Console dasselbe Konto verwenden, das Sie für Route 53 verwenden, ermöglicht Amazon SES Ihnen, Ihren DNS-Server sofort über die Amazon SES-Konsole zu aktualisieren.

Wenn Sie einen anderen DNS-Anbieter verwenden, variieren die Verfahren zum Aktualisieren der DNS-Datensätze je nachdem, welchen DNS- oder Webhosting-Anbieter Sie nutzen. Links zu der Dokumentation für mehrere gängige Anbieter werden in der nachfolgenden Tabelle aufgelistet. Diese Liste ist nicht vollständig und die Aufnahme in diese Liste ist keine Empfehlung oder Empfehlung für die Produkte oder Dienstleistungen eines Unternehmens. Wenn Ihr Anbieter in der Tabelle nicht aufgeführt ist, können Sie die Domäne wahrscheinlich mit Amazon SES verwenden.

DNS/Hosting-Anbieter	Link zur Dokumentation
GoDaddy	Hinzufügen eines TXT-Datensatzes
Dreamhost	Wie füge ich benutzerdefinierte DNS-Datensätze hinzu?
Cloudflare	Verwalten von DNS-Datensätzen in CloudFlare
HostGator	Verwalten von DNS-Datensätzen mit HostGator/eNOM
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC-Datensätze für meine Domain hinzu?
Names.co.uk	Ändern der DNS-Einstellungen Ihrer Domäne
Wix	Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto

Nach Abschluss der Verifizierung ändert sich der Domänenstatus in der Amazon SES Konsole von „Verifizierung ausstehend“ in „verifiziert“. Anschließend sendet eine Benachrichtigungs-E-Mail von Amazon SES.

8. Sie können nun mithilfe von Amazon SES E-Mails von allen Adressen der verifizierten Domäne senden. Zum Senden einer Test-E-Mail aktivieren Sie das Kontrollkästchen neben der verifizierten Domäne und wählen Send a Test Email aus.

Wenn die DNS-Einstellungen nicht korrekt aktualisiert wurden, erhalten Sie eine E-Mail von Amazon SES, die Sie über das Fehlschlagen der Domänenverifizierung informiert. Die Domäne zeigt den Status `failed` auf der Domänen-Registerkarte. Schließen Sie in diesem Fall die Schritte auf der Seite zur Fehlerbehebung unter [Häufige Probleme mit der Domänenverifizierung \(p. 509\)](#) ab. Nachdem Sie überprüft haben, dass Ihr TXT korrekt erstellt wurde, wählen Sie den Retry (Wiederholen)-Link neben der `failed`-Statusbenachrichtigung aus, um den Prozess zur Domänenverifizierung neu zu starten.

Amazon Auflisten von Domänen-Identitäten in Amazon SES

Führen Sie die folgenden Schritte durch, um Ihre verifizierten Domänen anzuzeigen.

So zeigen Sie Ihre verifizierten Domänen an

1. Wechseln Sie zu Ihrem [Verifizierte Domänenliste](#) oder führen Sie folgende Schritte aus, um zu dieser zu navigieren:
 - a. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
 - b. Wählen Sie im Navigationsbereich unter Identity Management die Option Domains aus.
2. Sie können in der Liste der verifizierten Domänen eine oder mehrere Domänen erweitern, um Details anzuzeigen.

Löschen einer Domänen-Identität in Amazon SES

Führen Sie die folgenden Schritte durch, um eine verifizierte Domäne zu entfernen.

So entfernen Sie eine verifizierte Domäne

1. Wechseln Sie zu Ihrem [Verifizierte Domänenliste](#) oder führen Sie folgende Schritte aus, um zu dieser zu navigieren:
 - a. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
 - b. Wählen Sie im Navigationsbereich unter Identity Management die Option Domains aus.
2. Aktivieren Sie das Kontrollkästchen neben der zu entfernenden Domäne und klicken Sie dann auf Remove.
3. Sie können von der entfernten Domäne keine E-Mails mehr senden.

Verifizieren einer Amazon SES S-Domänenverifizierung

überprüft Amazon SES regelmäßig den Status des Domännennachweises und widerruft diesen, wenn er nicht mehr gültig ist. Wenn Amazon SES die TXT-Datensatzinformationen nicht erkennt, die notwendig sind, um den Besitz einer Domäne zu bestätigen, erhalten Sie eine Warnung zur Amazon SES S-Domänenüberprüfung E-Mail von Amazon SES.

Wenn Sie die TXT-Datensatzinformationen innerhalb von 72 Stunden auf dem DNS-Server Ihrer Domain wiederherstellen, erhalten Sie eine Amazon SES Domain-Verifizierung, STÜRKUNGE-Mail von Amazon SES.

Note

Sie können die erforderlichen TXT-Datensatzinformationen in der Amazon SES Konsole mithilfe der folgenden Anweisungen prüfen. Wählen Sie im Navigationsbereich unter Identity Management die Option Domains aus. Erweitern Sie nicht nur die Liste der Domänen, sondern wählen Sie in der Liste die Domäne aus, um deren Verifikationseinstellungen wie den Namen und Wert des TXT-Datensatzes anzuzeigen.

Wenn Sie die TXT-Datensatzinformationen nicht innerhalb von 72 Stunden auf dem DNS-Server Ihrer Domäne wiederherstellen, erhalten Sie eine Amazon SES Domänenverifizierung VERSTREIBUNG-E-Mail von Amazon SES, wird die Domain aus der Liste der Verifizierte Absender auf der Domänen und Sie können von der Domäne nicht mehr senden.

Um eine Domäne, für die die Verifizierung aufgehoben wurde, erneut zu verifizieren, müssen Sie die Verifizierung vollständig neu durchführen, so als wäre es eine neue Domäne.

TXT-Datensätze zur Amazon SES E-Domänenverifizierung

Ihre Domäne ist mit einer Reihe von DNS (Domain Name System)-Datensätzen verknüpft, die Sie über Ihren DNS-Anbieter verwalten. Ein TXT-Datensatz ist eine Art von DNS-Datensatz, der zusätzliche Informationen zu Ihrer Domäne bereitstellt. Jeder TXT-Datensatz besteht aus einem Namen und einem Wert.

Wenn Sie die Domänenverifizierung mit der Amazon SES Konsole oder -API initiieren, gibt Amazon SES den Namen und Wert für den TXT-Datensatz vor. Beispiel: Wenn Ihre Domäne `example.com` sehen die von Amazon SES generierten TXT-Datensatz-Einstellungen in etwa wie im folgenden Beispiel gezeigt aus:

Name	Typ	Value
<code>_amazonses.example.com</code>	TXT	<code>pmBGN/7MjnfhTKUZ06Enqq1PeGUaOkw8lGhcfwefcHU=</code>

Fügen Sie einen TXT-Datensatz zum DNS-Server Ihrer Domäne mit dem angegebenen Name und Value. Die Amazon SES-Domänenverifizierung ist abgeschlossen, wenn Amazon SES erkennt, dass der TXT-Datensatz in den DNS-Einstellungen Ihrer Domäne vorhanden ist.

Note

Einige DNS-Anbieter hängen den Domännennamen automatisch an die Namen von DNS-Datensätzen an. Zur Vermeidung doppelter Domännennamen können Sie im DNS-Datensatz einen Punkt (.) an das Ende des Domännennamens einfügen oder Ihre Domäne aus dem Datensatznamen weglassen. Weitere Informationen finden Sie in der Dokumentation zu Ihrem DNS-Anbieter.

Wenn Ihr DNS-Anbieter Unterstriche in DNS-Datensatznamen nicht zulässt, können Sie `_amazonses` im Feld Name weglassen. In diesem Fall würde beim vorherigen Beispiel der TXT-Datensatzname `example.com` anstelle von `_amazonses.example.com` lauten. Damit der Datensatz leichter erkannt und einfacher verwaltet werden kann, können Sie dem Wert das Präfix `amazonses:` zuordnen. Im vorherigen Beispiel würde der Wert für den TXT-Datensatz `amazonses:pmBGN/7MjnfhTKUZ06Enqq1PeGUaOkw8lGhcfwefcHU=` lauten.

Note

In Amazon SES waren bis vor kurzem TXT-Datensätze mit zulässig. Amazonses ohne Unterstrich. Wenn Sie bereits eine Domäne verifiziert haben und der TXT-Datensatz enthält `amazonses` ohne Unterstrich, bleibt die Domäne verifiziert und Sie müssen keine Maßnahmen ergreifen. Für alle neuen Domänen, die Sie verifizieren, ist es aber erforderlich, dass `amazonses` im TXT-Datensatznamen entweder ein Unterstrich vorangestellt wird, oder dass `_amazonses` vollständig aus dem TXT-Datensatznamen entfernt wird.

Informationen zur Fehlerbehebung und Anweisungen für die Überprüfung der Einstellungen für die Domänenverifizierung finden Sie unter [Häufige Probleme mit der Domänenverifizierung \(p. 509\)](#).

Hinzufügen eines TXT-Datensatz zum DNS-Server der Domäne

Die Schritte zum Hinzufügen von TXT-Datensätzen zum DNS-Server Ihrer Domäne hängen davon ab, wer den DNS-Dienst bereitstellt. Ihr DNS-Anbieter kann Amazon Route 53 oder eine andere Domännennamen-Vergabestelle wie beispielsweise GoDaddy sein. Dieser Abschnitt enthält Verfahren für das Hinzufügen eines TXT-Datensatzes in Route 53 sowie allgemeine Verfahren für andere DNS-Anbieter.

Vorgehensweisen für Amazon Route 53

Wenn Sie beginnen [den Prozess der Überprüfung einer neuen Domain \(p. 66\)](#) Wenn Sie mit Amazon SES verwenden möchten, können Sie den TXT-Datensatz der Domänenverifizierung Ihrer Route 53 Konfiguration automatisch hinzufügen. Wenn Sie jedoch den TXT-Datensatz nicht automatisch hinzufügen, können Sie den TXT-Datensatz Ihrer Route 53 Konfiguration manuell hinzufügen, indem Sie das Verfahren in diesem Abschnitt abschließen.

So fügen Sie einen TXT-Datensatz zum DNS-Datensatz für Ihre Route 53-verwaltete Domäne hinzu

1. Öffnen der Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie unter Identity Management (Identitätsverwaltung) die Option Domänen aus.
3. Wählen Sie die Domäne aus, die Sie überprüfen möchten.
4. Erweitern Sie den Abschnitt Verifizierung. Kopieren Sie den Wert neben TXT-Wert.
5. Öffnen Sie die Route 53-Konsole unter <https://console.aws.amazon.com/route53/>.
6. Klicken Sie im Navigationsbereich auf Hosted Zones.
7. Wählen Sie die Domäne aus, der Sie einen TXT-Datensatz hinzufügen möchten.
8. Wählen Sie Create Record Set (Datensatz erstellen).
9. Für Routing-Richtlinie, wählen Sie Einfaches Routing. Klicken Sie auf und anschließend auf Weiter.
10. Wählen Sie Define simple record (Einfachen Datensatz definieren).
11. In der Definieren von einfachen Datensätzen Führen Sie im Bereich die folgenden Schritte aus:

- a. Für Datensatzname, geben Sie **_amazonses**.
 - b. Für Datenverkehr weiterleiten an, wählen Sie IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Fügen Sie dann im Textbereich den Wert des TXT-Datensatzes ein, den Sie aus der Amazon SES -Konsole kopiert haben.
 - c. Wählen Sie für den Record type (Datensatztyp) TXT.
 - d. Für TTL (Sekunden), Typ **1800**.
 - e. Wählen Sie Define simple record (Einfachen Datensatz definieren).
12. Warten Sie etwa 30 Minuten, bis der Datensatz vorschlägt. Klicken Sie dann auf der Registerkarte Domänen in der Amazon SES Konsole den Wert im Status neben der Domäne. Wenn der Status „pending verification“ (ausstehende Verifizierung) lautet, warten Sie weitere 30 Minuten und wählen Sie dann Refresh (↻) enthalten. Wiederholen Sie diesen Vorgang, bis der Wert in der Spalte Status "verified" (überprüft) lautet.

Generische Verfahren für andere DNS-Anbieter

Die Verfahren zum Hinzufügen von TXT-Datensätzen zu DNS-Konfigurationen variieren von Anbieter zu Anbieter. Spezifische Schritte finden Sie in der Dokumentation Ihres DNS-Anbieters. Die Verfahren in diesem Abschnitt bieten einen einfachen Überblick über die Schritte, die Sie beim Hinzufügen eines TXT-Datensatzes zur DNS-Konfiguration für Ihre Domäne ausführen.

So fügen Sie einen TXT-Datensatz zum DNS-Server der Domäne hinzu (allgemeines Verfahren)

1. Gehen Sie zur Verwaltungskonsole Ihres DNS-Anbieters und melden Sie sich bei Ihrem Konto an.
2. Suchen Sie nach der Seite zum Aktualisieren der DNS-Datensätze Ihrer Domäne. Möglicherweise hat diese Seite einen Namen, der etwa wie folgt aussieht: DNS-Datensätze, DNS-Zonendatei, oder Erweiterter DNS. Weitere Informationen finden Sie in der Dokumentation Ihres DNS-Anbieters.
3. Fügen Sie einen TXT-Datensatz mit dem von Amazon SES bereitgestellten Namen und Wert hinzu.

Wichtig

Einige DNS-Anbieter, wie z. B. GoDaddy, hängen den Domännennamen automatisch an das Ende von DNS-Datensätzen an. Wenn Sie einen Datensatz hinzufügen, der bereits den Domännennamen enthält (beispielsweise `_amazonses.example.com`) kann das zu einer Duplizierung des Domännennamens führen (beispielsweise `_amazonses.example.com.example.com`). Zur Vermeidung doppelter Domännennamen können Sie im DNS-Datensatz einen Punkt an das Ende des Domännennamens einfügen oder Ihre Domäne aus dem Datensatznamen weglassen. Weitere Informationen finden Sie in der Dokumentation Ihres DNS-Anbieters.

4. Speichern Sie Ihre Änderungen. Bis die Aktualisierung eines DNS-Datensatzes wirksam wird, können bis zu 48 Stunden vergehen, in der Regel erfolgt dies aber schneller. In dem Sie die in [Überprüfen der Einstellungen für die Domänenverifizierung \(p. 510\)](#) beschriebenen Schritte durchführen, können Sie bestätigen, dass der TXT-Datensatz korrekt veröffentlicht wurde.

Abrufen von AWS-Zugriffsschlüsseln

Nachdem Sie sich bei Amazon SES angemeldet haben, benötigen Sie AWS Zugriffsschlüssel, wenn Sie mit der Amazon SES -API auf Amazon SES zugreifen möchten, sei es direkt über die Abfrage (HTTPS) - Schnittstelle oder indirekt über eine [AWS SDK](#), die [AWS Command Line Interface](#), oder die [AWS Tools for Windows PowerShell](#). AWS-Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel.

Weitere Informationen zu den Arten von Sicherheitsschlüsseln, die Sie in Amazon SES verwenden können, finden Sie unter [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#). Weitere Informationen zum

Abrufen von AWS Zugriffsschlüsseln finden Sie unter [AWS Anmeldeinformationen](#) im Allgemeine AWS-Referenz.

Herunterladen eines AWS SDKs

Wenn Sie die Amazon SES S-API aufrufen möchten, ohne sich mit Details der unteren Ebene, beispielsweise dem Erstellen unformatierter HTTP-Anforderungen, beschäftigen zu müssen, können Sie ein AWS SDK verwenden. Die AWS SDKs stellen Funktionen und Datentypen bereit, die die Funktionalität von Amazon SES und anderen AWS -Services umfassen. Wechseln Sie zum [Herunterladen eines AWS SDKs zu SDKs](#).

Der Abschnitt "Erste Schritte" dieser Anleitung enthält Beispiele für das Senden einer E-Mail mit AWS SDKs für verschiedene Programmiersprachen. Weitere Informationen finden Sie unter [Senden einer E-Mail über Amazon SES mithilfe eines AWS -SDKs \(p. 34\)](#).

Einrichten 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 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.

Wenn Amazon SES die MAIL FROM-Domäne für die Nachrichten, die Sie senden, auf einen Standardwert setzt, es sei denn, Sie geben Ihre eigene Domäne 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?

Standardmäßig wird für Nachrichten, die über Amazon SES gesendet werden, eine Subdomäne von `amazonses.com` als MAIL FROM-Domäne. Die Sender Policy Framework (SPF) -Authentifizierung verifiziert diese Nachrichten erfolgreich, da die standardmäßige MAIL FROM-Domäne mit der Anwendung, die die E-Mail gesendet hat — in diesem Fall Amazon SES.

Obwohl diese Authentifizierungsstufe für viele Sender ausreicht, ziehen andere Sender es vor, als MAIL FROM-Domäne eine Domäne in ihrem Besitz einzustellen. Durch die Einrichtung einer benutzerdefinierten MAIL FROM-Domäne können Ihre E-Mails [Domain-based Message Authentication, Reporting and Conformance \(DMARC\) \(p. 154\)](#) entsprechen. Mit DMARC kann die Domäne eines Senders angegeben, dass von der Domäne gesendete E-Mails durch ein oder mehrere Authentifizierungssysteme geschützt sind.

Es gibt zwei Möglichkeiten, eine DMARC-Validierung zu erreichen: mithilfe von [Sender Policy Framework \(p. 141\)](#) (SPF) und [DomainKeys Identified Mail \(p. 142\)](#) (DKIM). Die einzige Möglichkeit, DMARC über SPF zu entsprechen, besteht darin, eine benutzerdefinierte MAIL FROM-Domäne zu verwenden, da die SPF-Validierung erfordert, dass die Domäne in der From-Adresse mit der MAIL FROM-Domäne übereinstimmt. Durch die Verwendung Ihrer eigenen MAIL FROM-Domäne haben Sie die Flexibilität, SPF, DKIM oder beide zu verwenden, um die DMARC-Validierung zu erzielen.

Auswählen einer MAIL FROM-Domäne

Die Subdomäne, die Sie für Ihre MAIL FROM-Domäne verwenden, muss die folgenden Anforderungen erfüllen:

- Die MAIL FROM-Domäne muss eine Subdomäne der verifizierten Identität (E-Mail-Adresse oder Domäne) sein, von der Sie E-Mails senden. Beispiel, `mail.example.com` Eine gültige MAIL FROM-Domäne für die Domäne `example.com`.
- Die MAIL FROM-Domäne sollte keine Domäne sein, von der Sie E-Mails senden. Wenn Sie die MAIL FROM-Domäne in einer Von-Adresse verwenden müssen, [Deaktivieren der E-Mail-Feedback-Weiterleitung](#) (p. 290) Wenn Sie Unzustellbarkeitsbenachrichtigungen über Amazon SNS Benachrichtigungen erhalten oder stellen Sie sicher, dass Ihre MAIL FROM-Domäne nicht die Zieladresse für die Feedback-Weiterleitung ist. Um die Zieladresse der Weiterleitung von Feedback per E-Mail festzustellen, lesen Sie den Abschnitt [E-Mail-Feedback-Weiterleitungsziel](#) (p. 291).
- Bei der MAIL FROM-Domäne sollte es sich nicht um eine Domäne handeln, auf der Sie E-Mails erhalten.

Konfigurieren der MAIL FROM-Domäne

Für die Einrichtung einer benutzerdefinierten MAIL FROM-Domäne müssen Sie Datensätze zur DNS-Konfiguration für die Domäne hinzufügen. Sie müssen einen MX-Datensatz veröffentlichen, damit Ihre Domäne die Unzustellbarkeits- und Beschwerdebenachrichtigungen erhält, die E-Mail-Anbieter Ihnen senden. Sie müssen auch einen SPF-Datensatz veröffentlichen, um nachzuweisen, dass Amazon SES berechtigt ist, E-Mails von Ihrer Domäne zu senden.

Sie können eine benutzerdefinierte MAIL FROM-Domäne für eine gesamte Domäne oder 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 auch eine benutzerdefinierte MAIL FROM-Domäne mit der API-Operation [SetIdentityMailFromDomain](#) konfigurieren.

Einrichten einer MAIL FROM-Domäne für eine verifizierte Domäne

Sie können eine MAIL FROM-Domäne für eine gesamte Domäne konfigurieren. Wenn Sie dies tun, verwenden alle Nachrichten, die Sie von Adressen in dieser Domäne senden, dieselbe MAIL FROM-Domäne.

So konfigurieren Sie eine verifizierte Domäne, um eine festgelegte MAIL FROM-Domäne zu verwenden

1. Öffnen der Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management die Option Domains aus.
3. Bestätigen Sie in der Liste der Domänen, dass die der MAIL FROM-Domäne übergeordnete Domäne verifiziert ist. Wenn die Domäne nicht verifiziert ist, führen Sie die Schritte unter [Überprüfen von Domänen in Amazon SES](#) (p. 65) aus, um die Domäne zu überprüfen. Wählen Sie andernfalls die Domäne aus und fahren Sie mit dem nächsten Schritt fort.
4. Wählen Sie unter MAIL FROM Domain (MAIL FROM-Domäne) die Option Set MAIL FROM Domain (MAIL FROM-Domäne festlegen) aus.
5. Führen Sie im Fenster Set MAIL FROM Domain (MAIL FROM-Domäne festlegen) die folgenden Schritte aus:
 - a. Geben Sie für MAIL FROM domain (MAIL FROM-Domäne) die Subdomäne ein, die Sie als MAIL FROM-Domäne verwenden möchten.
 - b. Wählen Sie für Behavior if MX record not found eine der folgenden Optionen aus:
 - Verwenden von `region.amazonses.com` FROM-MAIL— Wenn ein benutzerdefinierter MX-Eintrag der MAIL FROM-Domäne nicht ordnungsgemäß eingerichtet ist, verwendet Amazon SES eine Subdomäne von `amazonses.com`. Die Unterdomäne variiert je nach der AWS-Region, in der Sie Amazon SES verwenden.
 - Zurückweisen von Meldungen Wenn ein benutzerdefinierter MX-Eintrag der MAIL FROM-Domäne nicht ordnungsgemäß eingerichtet ist, gibt Amazon SES

eineMailFromDomainNotVerified-Fehler. E-Mails, die Sie von dieser Domäne aus senden möchten, werden automatisch abgelehnt.

- c. Wählen Sie Set MAIL FROM Domain aus. Es wird ein neues Fenster mit den MX- und SPF-Einträgen angezeigt, die Sie zur DNS-Konfiguration Ihrer Domäne hinzufügen müssen. Diese Datensätze verwenden die Formate in der folgenden Tabelle.

Name	Typ	Value
<code>subdomain.domain.com</code>	MX	10 feedback-smtp. <code>region</code> .amazonses.com
<code>subdomain.domain.com</code>	TXT	„v=spf1include:amazonses.com~all“

Ersetzen Sie in den vorherigen Datensätzen `subdomain.domain.com` durch Ihre MAIL FROM-Subdomäne und `region` durch den Namen der AWS-Region, in der Sie die MAIL FROM-Domäne verifizieren möchten (z. B. `us-west-2`, `us-east-1`, oder `eu-west-1`). Beachten Sie, dass der Wert des TXT-Datensatzes die Anführungszeichen enthalten muss.

Notieren Sie sich diese Werte und fahren Sie mit dem nächsten Schritt fort.

6. Veröffentlichen Sie als Nächstes einen MX-Eintrag im DNS-Server der benutzerdefinierten MAIL FROM-Domäne.

Important

Um erfolgreich eine benutzerdefinierte MAIL FROM-Domäne mit Amazon SES einzurichten, müssen Sie genau einen MX-Eintrag im DNS-Server Ihrer benutzerdefinierten MAIL FROM-Domäne veröffentlichen. Wenn die MAIL FROM-Domäne über mehrere MX-Einträge verfügt, wird die benutzerdefinierte MAIL FROM-Einrichtung mit Amazon SES fehlschlagen.

Wenn Route 53 den DNS-Service für Ihre MAIL FROM-Domäne bereitstellt und Sie bei der AWS Management Console unter dem gleichen Konto, das Sie für Route 53 verwenden, und wählen Sie Veröffentlichen von Datensätzen mit Route 53. 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. 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 wahrscheinlich dennoch eine MAIL FROM-Domäne einrichten. 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
GoDaddy	- MX-CODE Hinzufügen eines MX-Datensatzes - TXT Hinzufügen eines TXT-Datensatzes
DreamHost	- MX-CODE Wie ändere ich meine MX-Datensätze? - TXT Wie füge ich benutzerdefinierte DNS-Datensätze hinzu?
Cloudflare	MX-CODE Wie kann ich Mail- oder MX-Datensätze hinzufügen oder bearbeiten?

Name des DNS/Hosting-Anbieters	Link zur Dokumentation
	• TXT Verwalten von DNS-Datensätzen in CloudFlare
HostGator	• MX-CODE Ändern von MX-Datensätzen — Windows • TXT Verwalten von DNS-Datensätzen mit HostGator/eNOM
Namecheap	• MX-CODE Wie kann ich die für den Mail-Service benötigten MX-Datensätze einrichten? • TXT Wie füge ich TXT/SPF/DKIM/DMARC-Datensätze für meine Domain hinzu?
Names.co.uk	• MX-CODE Ändern der DNS-Einstellungen Ihrer Domäne • TXT Ändern der DNS-Einstellungen Ihrer Domäne
Wix	• MX-CODE Hinzufügen oder Aktualisieren von MX-Datensätzen in Ihrem Wix-Konto • TXT Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto

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 MAIL FROM-Domäne 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 auf der Registerkarte `gmail.com`-Domäne, da Sie die erforderlichen DNS-Einträge der Domäne nicht hinzufügen können).

So konfigurieren Sie eine verifizierte E-Mail-Adresse, um eine festgelegte MAIL FROM-Domäne zu verwenden

1. Öffnen der Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management die Option Email Addresses aus.
3. Bestätigen Sie in der Liste der E-Mail-Adressen, dass die E-Mail-Adresse, für die Sie eine benutzerdefinierte MAIL FROM-Domäne einrichten möchten, verifiziert ist. Wenn die E-Mail-Adresse nicht verifiziert ist, führen Sie die Schritte unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#) aus, um die E-Mail-Adresse zu überprüfen. Andernfalls wählen Sie die E-Mail-Adresse aus und fahren Sie mit dem nächsten Schritt fort.
4. Wählen Sie unter MAIL FROM Domain (MAIL FROM-Domäne) die Option Set MAIL FROM Domain (MAIL FROM-Domäne festlegen) aus.
5. Führen Sie im Fenster Set MAIL FROM Domain (MAIL FROM-Domäne festlegen) die folgenden Schritte aus:

- a. Geben Sie für MAIL FROM domain (MAIL FROM-Domäne) die Subdomäne ein, die Sie als MAIL FROM-Domäne verwenden möchten.
- b. Wählen Sie für Behavior if MX record not found eine der folgenden Optionen aus:
 - Verwenden von `region.amazonses.com` FROM-MAIL— Wenn ein benutzerdefinierter MX-Eintrag der MAIL FROM-Domäne nicht ordnungsgemäß eingerichtet ist, verwendet Amazon SES eine Subdomäne von `amazonses.com`. Die Unterdomäne variiert je nach der AWS-Region, in der Sie Amazon SES verwenden.
 - Zurückweisen von Meldungen Wenn ein benutzerdefinierter MX-Eintrag der MAIL FROM-Domäne nicht ordnungsgemäß eingerichtet ist, gibt Amazon SES eine `MailFromDomainNotVerified`-Fehler. E-Mails werden bei einem Sendeversuch von dieser Adresse automatisch abgelehnt.
- c. Wählen Sie Set MAIL FROM Domain aus. Es wird ein Fenster mit den MX- und SPF-Datensätzen angezeigt, die Sie der DNS-Konfiguration für die Domäne hinzufügen müssen, zu der die E-Mail-Adresse gehört. Diese Datensätze verwenden die Formate in der folgenden Tabelle.

Name	Typ	Value
<code>subdomain.domain.com</code>	MX	10 feedback-smtp. <code>region</code> .amazonses.com
<code>subdomain.domain.com</code>	TXT	„v=spf1include:amazonses.com~all“

Ersetzen Sie in den vorherigen Datensätzen `subdomain.domain.com` durch Ihre MAIL FROM-Subdomäne und `region` durch den Namen der AWS-Region, in der Sie die MAIL FROM-Domäne verifizieren möchten (z. B. `us-west-2`, `us-east-1`, oder `eu-west-1`). Beachten Sie, dass der Wert des TXT-Datensatzes die Anführungszeichen enthalten muss.

Notieren Sie sich diese Werte und fahren Sie mit dem nächsten Schritt fort.

6. Veröffentlichen Sie die DNS-Datensätze auf dem DNS-Server der benutzerdefinierten MAIL FROM-Domäne.

Important

Um erfolgreich eine benutzerdefinierte MAIL FROM-Domäne mit Amazon SES einzurichten, müssen Sie genau einen MX-Eintrag im DNS-Server Ihrer benutzerdefinierten MAIL FROM-Domäne veröffentlichen. Wenn die MAIL FROM-Domäne über mehrere MX-Einträge verfügt, wird die benutzerdefinierte MAIL FROM-Einrichtung mit Amazon SES fehlschlagen.

Wenn Route 53 den DNS-Service für Ihre MAIL FROM-Domäne bereitstellt und Sie bei der AWS Management Console unter dem gleichen Konto, das Sie für Route 53 verwenden, und wählen Sie Veröffentlichen von Datensätzen mit Route 53. 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. 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 wahrscheinlich dennoch eine MAIL FROM-Domäne einrichten. 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
GoDaddy	- MX-CODE Hinzufügen eines MX-Datensatzes - TXT Hinzufügen eines TXT-Datensatzes
DreamHost	- MX-CODE Wie ändere ich meine MX-Datensätze? - TXT Wie füge ich benutzerdefinierte DNS-Datensätze hinzu?
Cloudflare	- MX-CODE Wie kann ich Mail- oder MX-Datensätze hinzufügen oder bearbeiten? - TXT Verwalten von DNS-Datensätzen in CloudFlare
HostGator	- MX-CODE Ändern von MX-Datensätzen — Windows - TXT Verwalten von DNS-Datensätzen mit HostGator/eNOM
Namecheap	- MX-CODE Wie kann ich die für den Mail-Service benötigten MX-Datensätze einrichten? - TXT Wie füge ich TXT/SPF/DKIM/DMARC-Datensätze für meine Domain hinzu?
Names.co.uk	- MX-CODE Ändern der DNS-Einstellungen Ihrer Domäne - TXT Ändern der DNS-Einstellungen Ihrer Domäne
Wix	- MX-CODE Hinzufügen oder Aktualisieren von MX-Datensätzen in Ihrem Wix-Konto - TXT Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto

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 MAIL FAmazon 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 Zustand ändert, sendet Amazon SES eine Benachrichtigung an die E-Mail-Adresse, die mit Ihrem AWS Konto verknüpft ist.

Status	E-Mail-Sendeverhalten	Amazon SES Aktionen
Ausstehend	Verwendet benutzerdefinierte MAIL FROM-Fallback-Einstellung	Amazon SES versucht, den erforderlichen MX-Eintrag für 72 Stunden zu erkennen.

Status	E-Mail-Sendeverhalten	Amazon SES Aktionen
		Im Falle eines Fehlschlags ändert sich der Zustand zu "Failed".
Herzlichen Glückwunsch	Verwendet benutzerdefinierte MAIL FROM-Domäne	Amazon SES kontinuierlich, ob der erforderliche MX-Eintrag vorliegt.
TemporaryFailure	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".
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 der MAIL FROM-Domäne (p. 73) neu starten.

Einrichten von SPF-Datensätzen für Amazon SES

Ein SPF-Datensatz zeigt den ISPs an, dass Sie Amazon SES autorisiert haben, E-Mails von Ihrer Domäne zu senden. Wenn Sie Amazon SES nutzen, hängt die Entscheidung darüber, ob ein SPF-Datensatz veröffentlicht werden soll, davon ab, ob Ihre E-Mail lediglich einer SPF-Prüfung des empfangenen E-Mail-Servers bestehen muss, oder ob Sie möchten, dass die E-Mail weitere Anforderungen erfüllen muss, die notwendig sind, um die Domain-based Message Authentication, Reporting und Konformitätsauthentifizierung (DMARC) basierend auf SPF. Weitere Informationen finden Sie unter [Authentifizierung Ihrer E-Mails mit SPF in Amazon SES \(p. 141\)](#) .

Einrichten Ihrer SMTP-Anmeldeinformationen für Amazon SES

Um die Amazon SES SMTP-Schnittstelle zu verwenden, müssen Sie zunächst einen SMTP-Benutzernamen und ein entsprechendes Passwort erstellen. Informationen zum Erhalt Ihrer SMTP-Anmeldeinformationen finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen](#) (p. 95).

Important

Ihr SMTP-Benutzername und das Passwort unterscheiden sich von Ihrer AWS-Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Verwenden Sie nicht Ihre AWS Anmeldeinformationen für die Authentifizierung bei einem Amazon SES SMTP-Endpunkt. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen](#) (p. 18).

Verlassen der Amazon SES -Sandbox

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

Wir platzieren alle neuen Konten in der Amazon SESSandbox. Während sich Ihr Konto in der Sandbox befindet, können Sie alle Funktionen von Amazon SES nutzen. Solange sich Ihr Konto in der Sandbox befindet, gelten jedoch die folgenden Einschränkungen für Ihr Konto:

- Sie können nur E-Mail senden auf Überprüfen Sie, ob E-Mail-Adressen und Domänen vorhanden sind, oder [Amazon SES Postfachsimulator](#) (p. 198).
- Sie können E-Mails nur von verifizierten E-Mail-Adressen und Domänen senden.

Note

Diese Einschränkung gilt auch dann, wenn sich Ihr Konto nicht in der Sandbox befindet.

- Sie können innerhalb von 24 Stunden nur maximal 200 E-Mails versenden.
- Pro Sekunden kann nur 1 Nachricht verschickt werden.

Wenn sich Ihr Konto nicht in der Sandbox befindet, können Sie E-Mails an beliebige Empfänger senden – unabhängig davon, ob die Adresse des Empfängers oder der Domäne verifiziert wurde. Sie müssen jedoch weiterhin alle Identitäten überprüfen, die Sie als Adressen für "From" (Von), "Source" (Quelle), "Sender" (Absender) oder "Return-Path" (Rücksendepfad) verwenden.

Führen Sie die Verfahren in diesem Abschnitt durch, um anzufordern, dass Ihr Konto aus der Sandbox entfernt wird.

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 Amazon EC2-Instance entfernt wird. Weitere Informationen finden Sie unter [Wie entferne ich die Drosselung auf Port 25 von meiner EC2-Instance?](#) im AWS-Wissenszentrum.

So fordern Sie an, dass Ihr Konto aus der Amazon SES -Sandbox mit der AWS Management Console

1. Öffnen der Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Klicken Sie im Navigationsbereich unter Versand von E-Mails Wählen Sie Sendestatistiken.

3. Führen Sie Ihre Kontodetails, wählen Sie Bearbeiten Sie Ihre Kontodetails, wie in der folgenden Abbildung dargestellt.

Your account details



Your Amazon SES account has "sandbox" access in region the Amazon SES mailbox simulator and verified email addresses. **Learn more**.

Can't find your existing account settings? Your account may navigation bar.

Production Access	Sandbox
Mail type	none
Website URL	none
Use case description	none
Additional contact addresses	none
Preferred contact language	none

Edit your account details

4. Geben Sie in den modalen Kontodetails die folgenden Kontodetails ein:

Edit your account details

Provide your account details, including a description of how you plan to use email, to update your account. Choose Yes if you wish to enable production access.

Enable Production Access

☐ Yes

☒ No

Mail type

Transactional

Website URL

Use case description

Additional contact addresses

Preferred contact language

English

I agree to the [AWS S](#)

C

- Für Aktivieren des Produktionszugriffs, wählen Sie Ja oder .Nein. Wählen Sie aus der Sandbox nur aus, indem Sie Ja.

- Wählen Sie als Mail Type (E-Mail-Typ) den E-Mail-Typ aus, den Sie senden möchten. Wenn mehr als ein Wert zutrifft, wählen Sie die Option aus, die für die meisten der E-Mails gilt, die Sie senden möchten.
- Geben Sie als Website URL (Website-URL) die URL der Website ein. Durch die Bereitstellung dieser Informationen können wir besser einschätzen, welche Art von Inhalt Sie senden möchten.
- Für Anwendungsfall Erläutern Sie, wie Sie Amazon SES zum Senden von E-Mails verwenden möchten. Beantworten Sie möglichst die folgenden Fragen, damit wir Ihre Anfrage bearbeiten können:
 - Wie werden Sie Ihre Mailingliste zusammenstellen bzw. von wo erhalten Sie diese?
 - Wie werden Sie mit Beschwerden und unzustellbaren Nachrichten umgehen?
 - Wie können Empfänger sich gegen den Erhalt Ihrer E-Mail entscheiden?
 - Wie haben Sie die Senderate oder Sendequote ermittelt, die Sie in dieser Anfrage angegeben haben?
- 5. Für Zusätzliche Kontaktadressen, teilen Sie uns mit, wo Sie Mitteilungen über Ihr Konto erhalten möchten. Dies kann eine durch Kommas getrennte Liste mit bis zu 4 E-Mail-Adressen sein.
- 6. Für bevorzugte Kontaktsprache Wählen Sie unter, ob Sie in diesem Fall in der Kommunikation mit diesem Fall erhalten möchten Englisch oder .Japanisch.
- 7. Wählen Sie im Bereich die Option Zur Überprüfung einreichen.

Note

Sobald Sie eine Überprüfung Ihrer Kontodetails eingereicht haben, können Sie Ihre Daten erst bearbeiten, wenn die Überprüfung abgeschlossen ist.

Anstatt eine Produktionszugriffsanforderung mit dem AWS Management Console verwenden, können Sie die Anforderung stattdessen mit dem AWS CLI. Senden Sie Ihre Anfrage mit der AWS CLI hilfreich, wenn Sie Produktionszugriff für eine große Anzahl von Identitäten anfordern möchten oder wenn Sie die Einrichtung von Amazon SES automatisieren möchten.

So fordern Sie an, dass Ihr Konto aus der Amazon SES -Sandbox mit der AWS CLI

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](#).

- Geben Sie in der Befehlszeile folgenden Befehl ein:

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

Gehen Sie im vorhergehenden Befehl wie folgt vor:

- Ersetzen **TRANSAKTIONAL** Versenden Sie durch die Art der E-Mail, die Sie über Amazon SES senden möchten. Sie können entweder TRANSACTIONAL oder PROMOTIONAL angeben. Wenn mehr als ein Wert zutrifft, geben Sie die Option an, die für die meisten der E-Mails gilt, die Sie senden möchten.
- Ersetzen **https://example.com** Mit der URL Ihrer Website. Durch die Bereitstellung dieser Informationen können wir besser einschätzen, welche Art von Inhalt Sie senden möchten.

- Ersetzen **Anwendungsfall** Hier wird beschrieben, wie Sie Amazon SES zum Senden von E-Mails verwenden möchten. Beantworten Sie möglichst die folgenden Fragen, damit wir Ihre Anfrage bearbeiten können:
 - Wie werden Sie Ihre Mailingliste zusammenstellen bzw. von wo erhalten Sie diese?
 - Wie werden Sie mit Beschwerden und unzustellbaren Nachrichten umgehen?
 - Wie können Empfänger sich gegen den Erhalt Ihrer E-Mail entscheiden?
 - Wie haben Sie die Senderate oder Sendequote ermittelt, die Sie in dieser Anfrage angegeben haben?
- Ersetzen **info@example.com** mit den E-Mail-Adressen, an denen Sie Mitteilungen über Ihr Konto erhalten möchten. Dies kann eine durch Kommas getrennte Liste mit bis zu 4 E-Mail-Adressen sein.
- Ersetzen **EN** Mit Ihrer bevorzugten Sprache. Sie können Folgendes angeben: **EN** für Englisch oder **JP** für Japanisch.

Note

Sobald Sie eine Überprüfung Ihrer Kontodetails eingereicht haben, können Sie Ihre Daten erst bearbeiten, wenn die Überprüfung abgeschlossen ist.

Das AWS Support -Team wird innerhalb von 24 Stunden erstmals auf die Anforderung antworten.

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.

Wenn Ihr Anwendungsfall gegen unsere Richtlinien verstößt, können wir Ihrer Anfrage möglicherweise nicht nachkommen.

Prüfen des Sandbox-Status für Ihr Konto

Sie können mithilfe der Amazon SES Konsole prüfen, ob sich Ihr Konto noch in der Sandbox befindet.

So stellen Sie fest, ob sich Ihr Konto in der Sandbox befindet:

1. Öffnen der Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Email Sending (Senden von E-Mails) die Option Sending Statistics (Sendestatistiken) aus.
3. **UNDER**Ihre Kontodetails Sie sehen den Status Ihres Kontos.

Wenn Ihr Konto noch überprüft wird, zeigt ein Banner an, dass Ihr Konto noch überprüft wird. Ihre ProduktionszugriffStatus wird immer noch als Sandbox.

Your account details



Your account details are currently under review. [See case 7266](#)

Production Access

Sandbox

Mail type

Transactional

Website URL

<https://example.com>

Use case description

A description of how you plan to use A

Additional contact addresses

info@example.com

Preferred contact language

English

Das Banner spiegelt auch den Status Ihres Kontos wider, wenn Ihre Anforderung, aus der Sandbox zu wechseln, abgelehnt oder fehlgeschlagen ist.

Wenn Ihre Anfrage zum Verlassen der Sandbox erteilt wurde, wird Ihr Produktionszugriff-Status auf `Enabled` gesetzt. Dieser Status bedeutet, dass sich Ihr Konto in der aktuellen Region nicht mehr in der Sandbox befindet.

Your account details

Production Access	Enabled
Mail type	Transactional
Website URL	https://example.com
Use case description	A description of how you plan to use A
Additional contact addresses	info@example.com
Preferred contact language	English

[Edit your account details](#)

Sie können auch feststellen, ob sich Ihr Konto in der Sandbox befindet, indem Sie eine E-Mail an eine Adresse senden, die Sie nicht überprüft haben. Sofern sich Ihr Konto in der Sandbox befindet, erhalten Sie eine Fehlermeldung, die besagt, dass die Zieladresse nicht verifiziert wurde.

Konfigurieren von benutzerdefinierten Domänen zur Verarbeitung der Öffnungs- und Klicknachverfolgung

Wenn Sie [Ereignisveröffentlichung](#) (p. 313) Wenn Sie Öffnungs- und Klick-Ereignisse erfassen möchten, nimmt Amazon SES kleinere Änderungen an den von Ihnen gesendeten E-Mails vor. Um offene Ereignisse zu erfassen, fügt Amazon SES ein transparentes Bild mit einer Breite und Höhe von jeweils 1 Pixel unten zu jeder E-Mail hinzu. Dieses Bild hat einen eindeutigen Dateinamen für jede E-Mail und wird auf einem Server gehostet, der von Amazon SES betrieben wird. Zum Erfassen von Link-Klickereignissen ersetzt Amazon SES die Links in Ihren E-Mails mit Links zu einem Server, der von Amazon SES betrieben wird. Dadurch wird der Empfänger sofort an sein ausgewähltes Ziel weitergeleitet. Einige Amazon SES-Kunden möchten vielleicht ihre eigenen Domänen verwenden, anstatt Domänen, die Amazon SES gehören und von diesem betrieben werden, um eine zusammenhängendere Erfahrung für die Empfänger zu erzeugen.

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 zum Einrichten einer Subdomäne auf einem Server, der Ihnen gehört, um Benutzer automatisch an die von Amazon SES betriebenen Server für die Öffnungs- und Klicknachverfolgung weiterzuleiten. Es gibt zwei Schritte bei der Einrichtung dieser Domänen. Zuerst konfigurieren Sie die Subdomäne selbst und dann setzen Sie einen Konfigurationssatz ein, um die benutzerdefinierte Domäne zu verwenden. In diesem Abschnitt werden Verfahren für die Durchführung dieser beiden Schritte beschrieben.

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 zu senden, die Links enthalten, die das HTTPS-Protokoll verwenden, sollten Sie eine HTTPS-Domäne für die Verarbeitung von Öffnungs- und Klicknachverfolgungsereignissen verwenden.

Wenn Sie eine HTTPS-Subdomäne verwenden möchten, befolgen Sie stattdessen die Anleitung unter [Option 2: Konfigurieren einer HTTPS-Domäne \(p. 87\)](#).

So richten Sie eine HTTP-Subdomäne für die Verarbeitung von Öffnungs- und Klicklinks ein

1. Wenn Sie dies nicht bereits getan haben, erstellen Sie eine Subdomäne zur Verwendung für Öffnungs- und Klicknachverfolgungs-Links. Wir empfehlen, dass Sie eine Subdomäne erstellen, die speziell für die Verarbeitung dieser Links vorgesehen ist.
2. Überprüfen Sie, ob die Unterdomäne für die Verwendung mit Amazon SES geeignet. Weitere Informationen finden Sie unter [Überprüfen von Domänen in Amazon SES \(p. 65\)](#).
3. Ändern Sie die DNS-Datensatz für die Unterdomäne. Fügen Sie einen neuen CNAME-Datensatz im DNS-Datensatz hinzu, der Anforderungen an die Amazon SES S-Nachverfolgungsdomäne umleitet. An welche Adresse Sie umleiten, hängt von der AWS Region ab, in der Sie Amazon SES verwenden. Die folgende Tabelle enthält eine Liste der Nachverfolgungsdomänen für die AWS Regionen, in denen Amazon SES verfügbar ist.

AWS-Region	AWS Tracking-Domäne
US East (Ohio)	<code>r.us-east-2.awstrack.me</code>
US East (N. Virginia)	<code>r.us-east-1.awstrack.me</code>
US West (Oregon)	<code>r.us-west-2.awstrack.me</code>
Asia Pacific (Mumbai)	<code>r.ap-south-1.awstrack.me</code>
Asia Pacific (Seoul)	<code>r.ap-northeast-2.awstrack.me</code>
Asia Pacific (Singapore)	<code>r.ap-southeast-1.awstrack.me</code>
Asia Pacific (Sydney)	<code>r.ap-southeast-2.awstrack.me</code>
Asia Pacific (Tokyo)	<code>r.ap-northeast-1.awstrack.me</code>
Canada (Central)	<code>r.ca-central-1.awstrack.me</code>

AWS-Region	AWS Tracking-Domäne
Europe (Frankfurt)	<code>r.eu-central-1.awstrack.me</code>
Europe (Ireland)	<code>r.eu-west-1.awstrack.me</code>
Europe (London)	<code>r.eu-west-2.awstrack.me</code>
South America (São Paulo)	<code>r.sa-east-1.awstrack.me</code>
AWS GovCloud (US)	<code>r.us-gov-west-1.awstrack.me</code>

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-Domäne für die Nachverfolgung von Linkklicks verwenden. Um eine HTTPS-Domäne für die Nachverfolgung von Links einzurichten, müssen Sie einige zusätzliche Schritte ausführen, die über die für die [Einrichtung einer HTTP-Domäne \(p. 86\)](#) erforderlichen Schritte hinausgehen.

Note

Sie können nur eine HTTPS-Domäne für die Nachverfolgung von Linkklicks verwenden. Amazon SES unterstützt nur die Öffnungsnachverfolgung über HTTP-Domänen

So richten Sie eine HTTPS-Subdomäne für die Verarbeitung von Klicks ein

1. Erstellen Sie eine Subdomäne zur Verwendung für Klicknachverfolgungs-Links. Wir empfehlen, dass Sie eine Subdomäne erstellen, die speziell für die Verarbeitung dieser Links vorgesehen ist.
2. Überprüfen Sie, ob die Unterdomäne für die Verwendung mit Amazon SES geeignet ist. Weitere Informationen finden Sie unter [Überprüfen von Domänen in Amazon SES \(p. 65\)](#).
3. Erstellen Sie ein neues Konto mit einem Content Delivery Network (CDN), wie [Amazon CloudFront](#).
4. Konfigurieren Sie das CDN so, dass Anforderungen an die Amazon SES Nachverfolgungsdomäne geleitet werden. An welche Adresse Sie umleiten, hängt von der AWS Region ab, in der Sie Amazon SES verwenden. Die folgende Tabelle enthält eine Liste der Nachverfolgungsdomänen für die AWS Regionen, in denen Amazon SES verfügbar ist.

AWS-Region	AWS Tracking-Domäne
US East (Ohio)	<code>r.us-east-2.awstrack.me</code>
US East (N. Virginia)	<code>r.us-east-1.awstrack.me</code>
US West (Oregon)	<code>r.us-west-2.awstrack.me</code>
Asia Pacific (Mumbai)	<code>r.ap-south-1.awstrack.me</code>
Asia Pacific (Seoul)	<code>r.ap-northeast-2.awstrack.me</code>
Asia Pacific (Singapore)	<code>r.ap-southeast-1.awstrack.me</code>
Asia Pacific (Sydney)	<code>r.ap-southeast-2.awstrack.me</code>

AWS-Region	AWS Tracking-Domäne
Asia Pacific (Tokyo)	<code>r.ap-northeast-1.awstrack.me</code>
Canada (Central)	<code>r.ca-central-1.awstrack.me</code>
Europe (Frankfurt)	<code>r.eu-central-1.awstrack.me</code>
Europe (Ireland)	<code>r.eu-west-1.awstrack.me</code>
Europe (London)	<code>r.eu-west-2.awstrack.me</code>
South America (São Paulo)	<code>r.sa-east-1.awstrack.me</code>
AWS GovCloud (US)	<code>r.us-gov-west-1.awstrack.me</code>

5. Wenn Sie Amazon CloudFront als Ihr CDN verwenden, führen Sie die folgenden Schritte aus:
 - a. Klicken Sie auf der CloudFront Verteilungen Wählen Sie die Verteilung aus, die Ihrem CDN entspricht.
 - b. Wählen Sie auf der Registerkarte Behaviors das Standardverhalten und anschließend Edit aus.
 - c. Wählen Sie für Cache Based on Selected Request Headers die Option All aus.
 - d. Wählen Sie für Query String Forwarding and Caching die Option Forward all, cache based on all aus.
 - e. Fügen Sie Ihrer Distribution einen alternativen Domännennamen hinzu. Die von Ihnen verwendete Unterdomäne muss in Amazon SES überprüft werden. Weitere Informationen finden Sie unter [Konfigurieren alternativer Domännennamen in Verbindung mit HTTPS](#) im Entwicklerhandbuch für Amazon CloudFront.

Wenn Sie ein anderes CDN als CloudFront verwenden, müssen Sie möglicherweise ähnliche Schritte durchführen. Weitere Informationen finden Sie in der Dokumentation zum CDN.

6. Wenn Sie zur Verwaltung der DNS-Konfiguration für Ihre Domäne Route 53 verwenden und CloudFront als CDN, erstellen Sie in Route 53 einen Alias-Datensatz, der sich auf die CloudFront-Verteilung (z. B. `d1111111abcdef8.cloudfront.net`) enthalten. Weitere Informationen finden Sie unter [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.

7. 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.

Teil 2 Einen Konfigurationssatz einrichten, um auf eine benutzerdefinierte Domäne für die Öffnungs- und Klicknachverfolgung zu verweisen

Nach der Konfiguration Ihrer Domäne für die Verarbeitung von Umleitungen der Öffnungs- und Klicknachverfolgung müssen Sie ein Ereignisziel in einem Konfigurationssatz einrichten, um auf Ihre benutzerdefinierte Domäne zu verweisen. Schließen Sie diesen Schritt mit der Amazon SES Konsole oder der `CreateConfigurationSetTrackingOptions` API-Operation. Dieser Abschnitt enthält Verfahren für die Ausführung dieser Aufgaben mit der Amazon SES Konsole. Weitere Informationen über die Verwendung der API finden Sie unter [CreateConfigurationSetTrackingOptions](#) im [Amazon Simple Email Service API-Referenz](#).

So erstellen Sie ein neues Konfigurationssatz-Ereignisziel, das sich auf eine benutzerdefinierte Nachverfolgungsdomäne bezieht

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie in der Navigationsleiste auf der linken Seite des Bildschirms Configuration Sets aus.
3. Wählen Sie Create Configuration Set aus.
4. Geben Sie für Configuration Set Name einen Namen für den Konfigurationssatz ein und wählen Sie Create Configuration Set aus.
5. Aktivieren Sie in der Liste mit den Konfigurationssätzen das Kontrollkästchen neben dem im vorherigen Schritt erstellten Konfigurationssatz. Wählen Sie im Menü Actions die Option Edit.
6. Wählen Sie auf der Registerkarte Event Destinations für Add Destination den Ereigniszieltyp aus. Weitere Informationen zu den Optionen in diesem Menü finden Sie unter [Schritt 2: Ereignisziel hinzufügen \(p. 316\)](#).
7. Wählen Sie für Event types entweder Click, Open oder beide Optionen aus, abhängig von den Ereignistypen, die Sie nachverfolgen möchten.
8. Wählen Sie für Domain Use your own subdomain aus.
9. Wählen Sie für Select a verified domain die Domäne aus, die Sie für die Nachverfolgung von Öffnungs- und Klickereignissen verwenden möchten. Im Textfeld links neben den Menü können Sie optional eine Subdomäne der übergeordneten Domäne angeben.
10. Konfigurieren Sie die verbleibenden Optionen auf übliche Weise. Weitere Informationen zum Erstellen von Ereigniszielen finden Sie unter [Schritt 2: Ereignisziel hinzufügen \(p. 316\)](#).
11. Wählen Sie Save (Speichern) aus.

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 diese Kunden die öffentlichen Amazon SES Endpunkte verwenden.

Wenn Sie innerhalb dieser Einschränkungen arbeiten möchten, können Sie Amazon Virtual Private Cloud (Amazon VPC) verwenden. Mit Amazon VPC können Sie AWS Ressourcen in einem virtuellen Netzwerk bereitstellen, das in einem isolierten Bereich der AWS Cloud existiert. Weitere Informationen über Amazon VPC finden Sie im[Amazon VPC Benutzerhandbuch](#).

Um Amazon SES mit Amazon VPC zu verwenden, müssen Sie zunächst eine Amazon EC2 Instance in der VPC Ihrer Organisation erstellen. Sie können dann eine Verbindung zu dieser Instance herstellen und sie verwenden, um E-Mails über Amazon SES zu senden. Dieser Abschnitt enthält Anweisungen zum Konfigurieren Ihrer Amazon EC2 Instance und zum Erstellen eines Amazon VPC Endpunkts für Amazon SES.

Note

Standardmäßig beschränkt Amazon Elastic Compute Cloud (Amazon EC2) den E-Mail-Verkehr über Port 25. Um Zeitüberschreitungen beim Versenden 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 Einschränkung auf Port 25 von meiner Amazon EC2 Instance oder der AWS Lambda Funktion?](#)im AWS-Wissenszentrum. Alternativ können Sie einen anderen Port (z. B. 587 oder 2587) verwenden, um dieses Problem zu vermeiden.

Prerequisites

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

- Erstellen Sie eine Virtual Private Cloud. Die entsprechenden Verfahren sind unter beschrieben. [Erste Schritte mit IPv4 für Amazon VPC](#).
- Starten Sie eine Amazon EC2 Instance in Ihrer VPC. Weitere Informationen finden Sie unter [Starten einer EC2-Instance in Ihrer Standard-VPC](#).

Einrichten von Amazon SES in Amazon VPC

Die Einrichtung eines VPC Endpunkts zur Verwendung mit Amazon SES besteht aus einigen wenigen separaten Schritten. Zuerst müssen Sie die private IP-Adresse der Amazon EC2 Instance identifizieren, die Sie mit dem VPC Endpunkt verwenden möchten. Als nächstes erstellen Sie eine Sicherheitsgruppe, die es der Instance erlaubt, mit SMTP-Ports zu kommunizieren. Danach erstellen Sie einen VPC Endpunkt für Amazon SES. Schließlich testen Sie die Verbindung zum VPC-Endpunkt, um sicherzustellen, dass dieser ordnungsgemäß konfiguriert ist.

Schritt 1: Suchen Sie die private IP-Adresse Ihrer Amazon EC2 Instance

Zum Einrichten einer Amazon EC2 Instance für die Verwendung eines Amazon SES VPC Endpunkts müssen Sie zunächst die private IP der Instance suchen. Sie verwenden diese IP-Adresse in einem späteren Schritt.

So suchen Sie die private IP einer Amazon EC2 Instance

1. Öffnen Sie die Amazon EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Navigationsbereich unter Instances die Option Instances.
3. Wählen Sie in der Liste der Amazon EC2 Instances die Instance aus, die Sie für die Verbindung mit dem VPC Endpunkt verwenden möchten.
4. Kopieren Sie im Detailbereich unten auf dem Bildschirm auf der Registerkarte Description (Beschreibung) die IP-Adresse neben Private IP.

Schritt 2: Erstellen der Sicherheitsgruppe

In Amazon EC2 wird ein-SicherheitsgruppeHier können Sie die ein- und ausgehende Kommunikation zu und von Ihrer VPC steuern. In diesem Schritt erstellen Sie eine Sicherheitsgruppe, die die Amazon EC2 Instance mit SMTP-Endpunkten kommunizieren lässt.

So erstellen Sie die Sicherheitsgruppe

1. Klicken Sie im Navigationsbereich der Amazon EC2 Konsole unter Netzwerk & Sicherheit, wählen Sie Sicherheitsgruppen.
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.
 - Für VPC Wählen Sie die VPC aus, in der Sie Amazon SES verwenden möchten.

Wenn Sie fertig sind, ähnelt der Abschnitt Basic details (Grundlegende Angaben) dem Beispiel in der folgenden Abbildung.

Basic details

Security group name [Info](#)

VPCEndpointSecurityGroup

Name cannot be edited after creation.

Description [Info](#)

Security group for Amazon SES VPC endpoint

VPC [Info](#)

vpc-example ▼

4. Wählen Sie unter Inbound rules (Regeln für eingehenden Datenverkehr) die Option Add rule (Regel hinzufügen).
5. Führen Sie unter Inbound rule 1 (Regel 1 für eingehenden Datenverkehr) die folgenden Schritte aus:
 - 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. Sie können eine der folgenden Portnummern verwenden: **25**, **465**, **587**, **2465** oder **2587**.
 - Wählen Sie für den Source type (Quellentyp) die Option Custom (Benutzerdefiniert).
 - Für Source Geben Sie die private IP Ihrer Amazon EC2 Instance ein (d. h. die Adresse, die Sie zuvor gefunden haben).
6. (Optional) Wenn Sie für weitere Ports eine Regel für eingehenden Datenverkehr hinzufügen möchten, wählen Sie erneut Add rule (Regel hinzufügen). Wiederholen Sie dann den vorherigen Schritt, um weitere Ports hinzuzufügen. Sie können Regeln für eine oder alle Portnummern erstellen, die im vorherigen Schritt aufgeführt sind.
7. Wenn Sie fertig sind, wählen Sie Create security group (Sicherheitsgruppe erstellen).

Schritt 3: Erstellen des VPC-Endpunkts

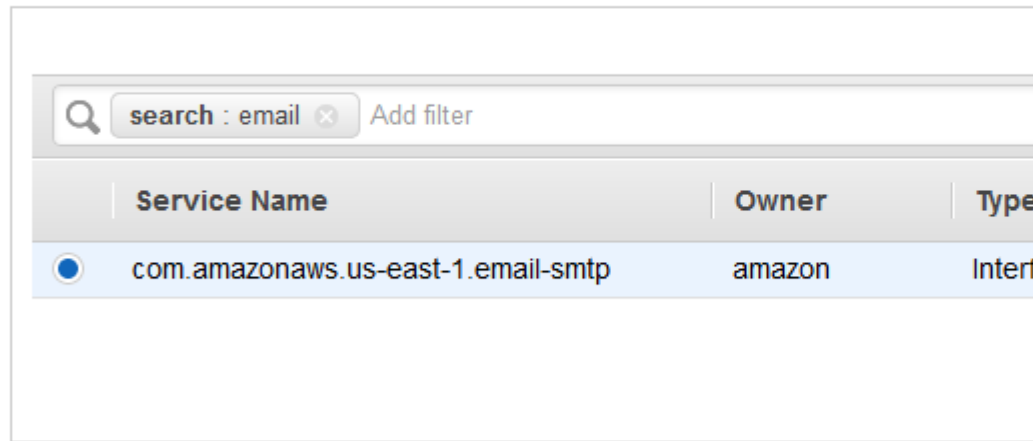
In Amazon VPC wird ein VPC-Endpunkt so verbinden Sie Ihre VPC mit unterstützten AWS -Services. In diesem Fall konfigurieren Sie Amazon VPC so, dass Ihre Amazon EC2 -Sicherheitsgruppe eine Verbindung mit Amazon SES herstellen kann.

So erstellen Sie den VPC Endpunkt

1. Öffnen Sie die Amazon VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie unter Virtual Private Cloud die Option Endpoints (Endpunkte) aus.
3. Klicken Sie auf Create Endpoint.
4. Wählen Sie auf der Seite Create Endpoint (Endpunkt erstellen) für Service category (Servicekategorie) die Option AWS-Services aus.

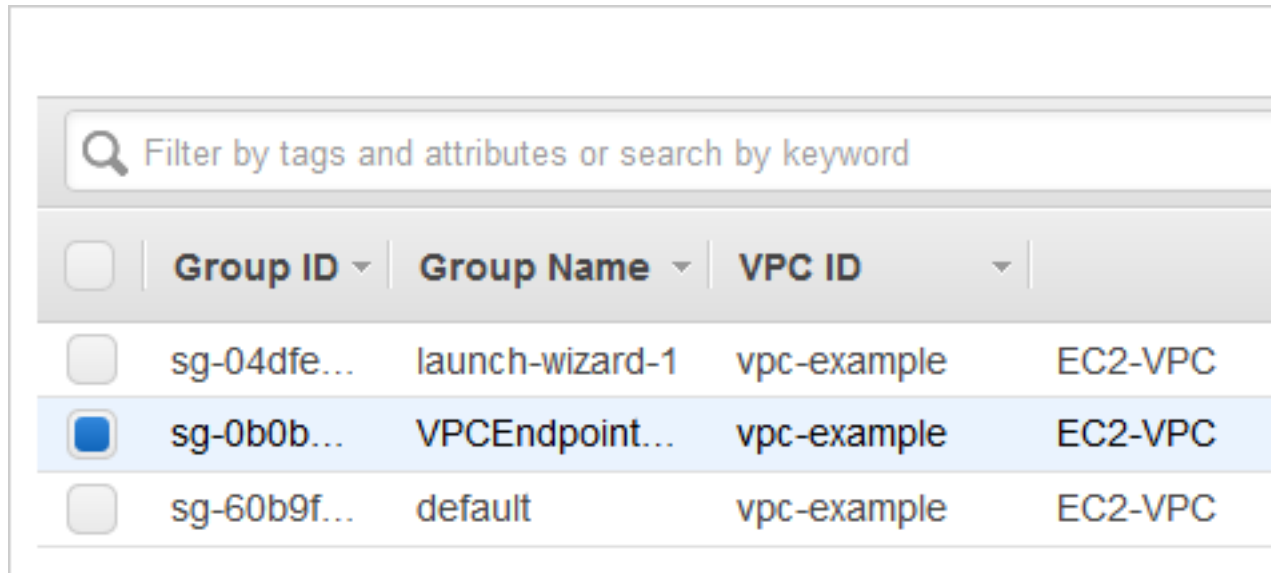
5. Verwenden Sie unter Service Name (Service-Name) das Suchfeld, um – wie in der folgenden Abbildung dargestellt – nach „E-Mail“ zu suchen.

Service Name `com.amazonaws.us-east-1.email-smtp` ⓘ

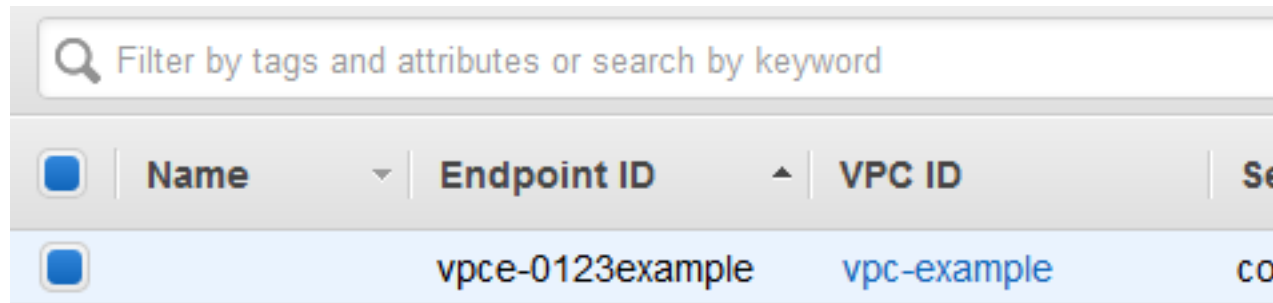


Wählen Sie das Symbol `email-smtp` für Ihre aktuelle AWS Region.

6. Wählen Sie für VPC die Virtual Private Cloud, die Sie verwenden möchten.
7. Wählen Sie unter Security group (Sicherheitsgruppe) die Sicherheitsgruppe aus, die Sie zuvor erstellt haben (s. folgende Abbildung).



8. Wählen Sie Create endpoint. 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 „available“ (verfügbar) (s. folgende Abbildung).



Schritt 4: Testen der Verbindung zum VPC Endpunkt

Wenn Sie die Konfiguration des VPC-Endpunkts abgeschlossen haben, sollten 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. Stellen Sie eine Verbindung zu Ihrer Amazon EC2-Instance her.

Weitere Informationen zum Verbinden mit Linux-Instances finden Sie unter [Herstellen einer Verbindung zur Linux-Instance](#) im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Weitere Informationen zum Verbinden mit Windows-Instances finden Sie unter [Erste Schritte](#) im Windows Amazon EC2 Benutzerhandbuch für Windows-Instances.

2. Senden Sie eine Test-E-Mail, indem Sie das Verfahren unter [Verwenden der Befehlszeile zum Senden von E-Mails mithilfe der Amazon SES -SMTP-Schnittstelle](#) (p. 115) abschließen.

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 [Überprüfen von Identitäten in Amazon SES](#) (p. 52).

E-Mail-Versandmethoden in Amazon SES

Sie können eine E-Mail mit Amazon Simple Email Service (Amazon SES) über die Amazon SES-Konsole, 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 finden Sie unter [Amazon SES – Preise](#).

- Wenn Sie ein Softwarepaket, eine Anwendung oder eine Programmiersprache, das bzw. die SMTP-fähig ist, zum Senden von E-Mails über Amazon SES verwenden oder Amazon SES in Ihren vorhandenen Mail-Server integrieren möchten, verwenden Sie die Amazon SES -SMTP-Schnittstelle. Weitere Informationen finden Sie unter [Senden von E-Mails über die Amazon SES SMTP-Schnittstelle](#) (p. 94) .
- 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](#) (p. 120) .

Bevor Sie E-Mails senden, lesen Sie nach unter [Einrichten von E-Mail mit Amazon SES](#) (p. 50).

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 erhält die beabsichtigte E-Mail. Wir empfehlen daher, dass Sie eine E-Mail nur jeweils an einen Empfänger senden.

Senden von E-Mails über die Amazon SES SMTP-Schnittstelle

Sie können die Simple Mail Transfer Protocol (SMTP) -Schnittstelle oder die Amazon SES S-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 \(p. 120\)](#). 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 -SMTP-Schnittstelle von Amazon SES herzustellen. In diesem Abschnitt wird erklärt, wie Sie Ihre -SMTP-Anmeldeinformationen erhalten, 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.

Note

Lösungen für häufige Probleme, die auftreten können, wenn Sie Amazon SES über die SMTP-Schnittstelle verwenden, finden Sie unter [Amazon SES SMTP-Probleme \(p. 518\)](#).

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

- Ein AWS-Konto. Weitere Informationen finden Sie unter [Registrieren bei AWS \(p. 51\)](#).
- Die SMTP-Endpunktadresse. Eine Liste der Amazon SES SMTP-Endpunkte finden Sie unter [Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt \(p. 100\)](#).
- Portnummer der SMTP-Schnittstelle. Die Portnummer variiert je nach Verbindungsmethode. Weitere Informationen finden Sie unter [Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt \(p. 100\)](#).
- 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 einen Benutzernamen und ein Passwort für jede Region.

Important

Ihr SMTP-Benutzername und das Passwort stimmen nicht mit Ihrem AWS Zugriffsschlüssel oder den Anmeldeinformationen überein, mit denen Sie sich bei der Amazon SES-Konsole anmelden. Weitere Informationen dazu, wie Sie Ihren SMTP-Benutzernamen und das Passwort erstellen, finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#).

- Client-Software, die mithilfe von Transport Layer Security (TLS) kommunizieren kann. Weitere Informationen finden Sie unter [Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt \(p. 100\)](#).
- Eine E-Mail-Adresse, die Sie mit Amazon SES verifiziert haben. Weitere Informationen finden Sie unter [Überprüfen von Identitäten in Amazon SES \(p. 52\)](#).
- Höhere Sendekontingente, wenn Sie große Mengen E-Mails senden möchten. Weitere Informationen finden Sie unter [Verwalten Ihrer Amazon SES Versandkontingente \(p. 156\)](#).

Dann können Sie Ihre E-Mails senden, indem Sie wie folgt vorgehen:

- Weitere Informationen zum Konfigurieren SMTP-fähiger Software für das Senden von E-Mails über die -SMTP-Schnittstelle von Amazon SES finden Sie unter [Senden von E-Mails über Amazon SES mit Softwarepaketen \(p. 100\)](#).
- Informationen zum Programmieren einer Anwendung für das Senden von E-Mails über Amazon SES finden Sie unter [Senden von E-Mails über Amazon SES aus Ihrer Anwendung \(p. 102\)](#).
- 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 \(p. 102\)](#).
- 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 \(p. 113\)](#).

Eine Liste der SMTP-Antwort-Codes finden Sie unter [Von Amazon SES zurückgegebene SMTP-Antwortcodes \(p. 519\)](#).

E-Mail-Informationen zur Verfügung zu stellen

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 eine Quelladresse, eine Zieladresse und Nachrichtendaten erforderlich.

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 einen Amazon SES SMTP-Benutzernamen und ein Passwort für den Zugriff auf die Amazon SES SMTP-Schnittstelle.

Die Anmeldeinformationen, die Sie für das Senden von E-Mails über die Amazon SES SMTP-Schnittstelle verwenden, sind für jede AWS Region eindeutig. Wenn Sie die Amazon SES SMTP-Schnittstelle zum Senden von E-Mails in mehr als einer Region verwenden, müssen Sie [Generieren eines Satzes von SMTP-Anmeldeinformationen \(p. 95\)](#) für jede Region, die Sie verwenden möchten.

Ihr SMTP-Kennwort unterscheidet sich von Ihrem geheimen AWS Zugriffsschlüssel. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#).

Abrufen von Amazon SES SMTP-Anmeldeinformationen über die Amazon SES-Konsole

Wenn Sie SMTP-Anmeldeinformationen mithilfe der Amazon SES Konsole generieren, erstellt die Amazon SES-Konsole einen IAM-Benutzer mit den entsprechenden Richtlinien zum Aufrufen von Amazon SES und stellt Ihnen die SMTP-Anmeldeinformationen für diesen Benutzer bereit.

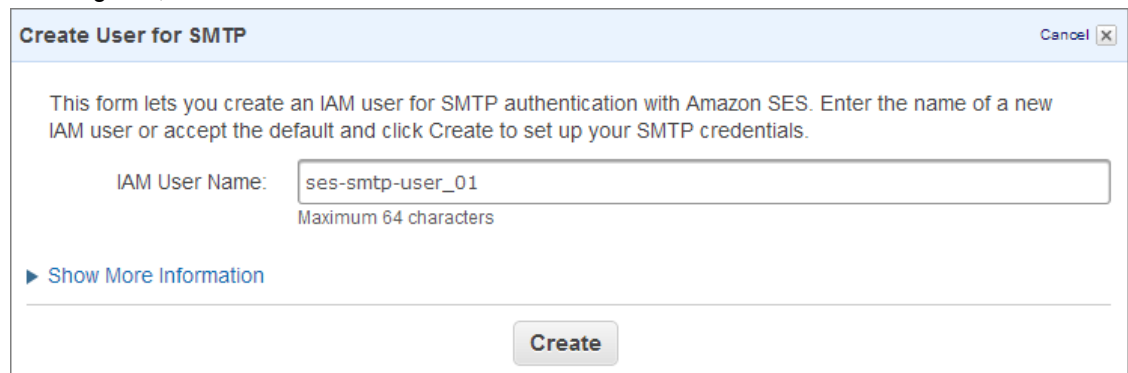
Requirement

Ein IAM-Benutzer kann Amazon SES SMTP-Anmeldeinformationen erstellen, die Richtlinie des IAM-Benutzers muss ihnen jedoch die Berechtigung zur Nutzung von IAM selbst erteilen, da die Amazon SES SMTP-Anmeldeinformationen mit IAM erstellt werden. Ihre IAM-Richtlinie muss zulassen, dass Sie die folgenden IAM-Aktionen durchführen: `iam:ListUsers`, `iam:CreateUser`, `iam:CreateAccessKey`, und `iam:PutUserPolicy`. Wenn Sie versuchen, Amazon SES -SMTP-Anmeldeinformationen mithilfe

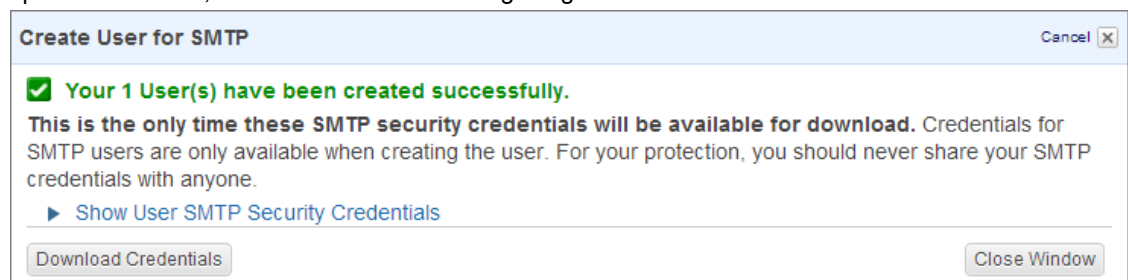
der Konsole zu erstellen und Ihr IAM-Benutzer nicht über diese Berechtigungen verfügt, wird bezüglich Ihres Kontos die Fehlermeldung „not authorized to perform iam:ListUsers“ (nicht zur Durchführung von iam:ListUsers) angezeigt.

So erstellen Sie Ihre SMTP-Anmeldeinformationen

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Klicken Sie im Navigationsbereich auf SMTP Settings.
3. Wählen Sie im Inhaltsbereich Create My SMTP Credentials aus.
4. Geben Sie unter Create User for SMTP (Benutzer für SMTP erstellen) einen Namen für Ihren Benutzer ein. Alternativ können Sie den Standardwert verwenden, der in diesem Feld bereitgestellt wird. Wenn Sie fertig sind, klicken Sie auf Create.



5. Wählen Sie die Option Show User SMTP Credentials. Ihre SMTP-Anmeldeinformationen werden auf dem Bildschirm angezeigt. Laden Sie diese Anmeldeinformationen herunter oder kopieren Sie sie und speichern Sie sie an einem sicheren Ort, da Sie Ihre Anmeldeinformationen nicht anzeigen oder speichern können, nachdem Sie dieses Dialogfeld geschlossen haben.



6. Wählen Sie Close Window aus.

Sie können eine Liste der vorhandenen SMTP-Anmeldeinformationen anzeigen, die Sie mit diesem Verfahren erstellt haben, indem Sie die IAM-Konsole aufrufen unter <https://console.aws.amazon.com/iam/>. Wählen Sie im Navigationsbereich unter Zugriffsverwaltung die Option Benutzeraus. Suchen Sie über die Suchleiste alle Benutzer, 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 <https://docs.aws.amazon.com/IAM/latest/UserGuide/Managing IAM-Benutzer> im Handbuch IAM — Erste Schritte.

Wenn Sie Ihre SMTP-Anmeldeinformationen drehen möchten, führen Sie das oben genannte Verfahren aus, um einen neuen Satz von SMTP-Anmeldeinformationen zu generieren. Testen Sie anschließend die neuen Anmeldeinformationen, um sicherzustellen, dass sie wie erwartet funktionieren. Löschen Sie schließlich den IAM-Benutzer, der den alten SMTP-Anmeldeinformationen in der IAM-Konsole

zugeordnet ist. Weitere Informationen zum Löschen von Benutzern in IAM finden Sie unter [Verwalten von Benutzern](#) im IAM-Benutzerhandbuch.

Abrufen von SMTP-Anmeldeinformationen von Amazon SES durch die Konvertierung vorhandener

Wenn Sie einen IAM-Benutzer haben, den Sie mithilfe der IAM-Schnittstelle eingerichtet haben, können Sie die Amazon SES SMTP-Anmeldeinformationen des Benutzers aus seinen AWS Anmeldeinformationen abrufen.

Important

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

Damit der IAM-Benutzer E-Mails über die Amazon SES SMTP-Schnittstelle senden kann, müssen Sie die beiden folgenden Schritte ausführen:

- Leiten Sie die SMTP-Anmeldeinformationen des Benutzers aus seinen AWS-Anmeldeinformationen mithilfe des Algorithmus in diesem Abschnitt ab. Da Sie von AWS Anmeldeinformationen ausgehen, entspricht der SMTP-Benutzername der AWS-Zugriffsschlüssel-ID, sodass Sie nur das SMTP-Passwort generieren müssen.
- Weisen Sie die dem IAM-Benutzer die folgenden Richtlinien zu:

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

Weitere Informationen zur Verwendung von Amazon SES mit IAM finden Sie unter [Steuern des Zugriffs auf Amazon SES \(p. 431\)](#).

Note

Sie können zwar Amazon SES SMTP-Anmeldeinformationen für alle IAM-Benutzer generieren, allerdings empfehlen wir, dass Sie bei der Generierung Ihrer SMTP-Anmeldeinformationen einen separaten IAM-Benutzer 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 einen Algorithmus, der einen geheimen AWS Zugriffsschlüssel in ein Amazon SES SMTP-Passwort konvertiert.

```
// 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 einen geheimen AWS Zugriffsschlüssel mit Python in ein Amazon SES SMTP-Passwort konvertieren können.

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)
    'sa-east-1',       # South America (Sao Paulo)
    'us-gov-west-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 for an IAM user 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 dann in der Befehlszeile 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 `Pfad/zu/` Mit dem Pfad zum Speicherort, an dem Sie gespeichert haben `smtp_credentials_generate.py`.
- Ersetzen `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` mit dem geheimen Zugriffsschlüssel, den Sie in ein SMTP-Kennwort konvertieren möchten.
- Ersetzen `us-east-1` Verwenden Sie die AWS Region, in der Sie die SMTP-Anmeldeinformationen verwenden möchten.

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

Um dieses Skript zu verwenden, speichern Sie zuerst den vorhergehenden Code als `smtp_credentials_generate.py`. Führen Sie dann in der Befehlszeile 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 `Pfad/zu/` Mit dem Pfad zum Speicherort, an dem Sie gespeichert haben `smtp_credentials_generate.py`.
- Ersetzen `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` Wenn Sie den zu konvertierenden geheimen -Zugriffsschlüssel verwenden möchten.
- Ersetzen `us-east-1` Verwenden Sie die AWS Region, in der Sie die SMTP-Anmeldeinformationen verwenden möchten.

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

Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt

Um E-Mails über die Amazon SES S-SMTP-Schnittstelle zu senden, stellen Sie eine Verbindung mit einem SMTP-Endpunkt her. Eine vollständige Liste der Amazon SES S-SMTP-Endpunkte finden Sie unter [Amazon Simple Email Service-Endpunkte und -kontingente](#) im Allgemeinen AWS-Referenz.

Der SMTP-Endpunkt von Amazon SES SMTP 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.

Note

Standardmäßig beschränkt Amazon Elastic Compute Cloud (Amazon EC2) den E-Mail-Verkehr über Port 25. Um Zeitüberschreitungen beim Versenden 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 Einschränkung auf Port 25 von meiner Amazon EC2 Instance oder der AWS Lambda Funktion?](#) im AWS-Wissenszentrum. Alternativ können Sie einen anderen Port verwenden oder eine [Amazon VPC Endpunkt](#) (p. 89).

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 S-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 mit 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 -SMTP-Schnittstelle von Amazon SES konfigurieren. Anweisungen zum Konfigurieren von SMTP für ein bestimmtes Softwarepaket finden Sie in der Dokumentation zu dieser Software.

Im folgenden Vorgang wird das Einrichten der -Sendung von Amazon SES in JIRA, einer gängigen Lösung für die Problemverfolgung, gezeigt. 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 die Option Mail Servers aus.
5. Klicken Sie auf Configure new SMTP mail server.
6. Füllen Sie im Formular Add SMTP Mail Server 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 bei Amazon SES verifizieren, bevor Sie von ihr senden können. Weitere Informationen zur Verifizierung finden Sie unter [Überprüfen von Identitäten in Amazon SES \(p. 52\)](#).
 - c. Email prefix – Eine Zeichenfolge, die JIRA vor dem Senden jeder Betreffzeile voranstellt.
 - d. Protocol – Wählen Sie SMTP aus.

Note

Wenn Sie mit dieser Einstellung keine Verbindung zu Amazon SES herstellen können, versuchen Sie es mit SECURE_SMTP.

- e. Host Name (Hostname)—finden Sie unter [Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt \(p. 100\)](#) Eine Liste der Amazon SES TP-Endpunkte finden Sie unter. Wenn Sie beispielsweise den Amazon SES Endpunkt in der Region USA West (Oregon) einsetzen 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. Username – Ihr SMTP-Benutzername.
- i. Password – Ihr SMTP-Passwort.

Einstellungen für TLS Wrapper werden unten gezeigt.

The screenshot shows the JIRA Administration interface. The left sidebar has a 'Mail' section with links to 'Mail Servers', 'Mail Queue', and 'Send E-mail'. The main content area is titled 'Update SMTP Mail Server' and contains the following fields:

- Name ***: Amazon SES (The name of this server within JIRA.)
- Description**: (Empty text box)
- From address ***: bob@example.com (The default address this server will use to send emails from.)
- Email prefix ***: JIRA (This prefix will be prepended to all outgoing email subjects.)
- Server Details**: Enter either the host name of your SMTP server or the JNDI location of a javax.mail.Session object to use.
- SMTP Host**:
 - Protocol**: SMTP (Dropdown menu)
 - Host Name ***: .us-east-1.amazonaws.com (The SMTP host name of your mail server.)
 - SMTP Port**: 465 (Optional - SMTP port number to use. Leave blank for default: (defaults: SMTP - 25, SMTPS - 465).)
 - Timeout**: 10000 (Timeout in milliseconds - 0 or negative values indicate infinite timeout. Leave blank for default (10000 mSecs).)
 - TLS**: ☒ (Optional - the mail server requires the use of TLS security.)

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.

Senden von E-Mails über Amazon SES aus Ihrer Anwendung

Viele Programmiersprachen unterstützen das Senden von E-Mails über SMTP. Diese Funktion kann in die Programmiersprache selbst integriert sein oder als Add-On, Plug-In oder Bibliothek zur Verfügung gestellt werden. Sie können diese Funktion nutzen, indem Sie E-Mails über Amazon SES aus Anwendungsprogrammen senden, die Sie schreiben.

Beispiele in C# und Java finden Sie unter [Programmatisches Senden einer E-Mail über die Amazon SES - SMTP-Schnittstelle](#) (p. 24) im Abschnitt mit den ersten Schritten.

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 beliebiger MTAs für das Senden von E-Mails mit der Amazon SES SMTP-Schnittstelle.

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

Themen

- [Integrieren von Amazon SES mit Postfix](#) (p. 103)
- [Integrieren von Amazon SES mit Sendmail](#) (p. 106)
- [Integrieren von Amazon SES in IIS-SMTP-Server von Microsoft Windows](#) (p. 110)
- [Integration von Amazon SES mit Exim](#) (p. 111)

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.

Prerequisites

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

- Deinstallieren Sie Sendmail, wenn es bereits auf Ihrem System installiert ist. Das Verfahren für die Ausführung dieses Schritts variiert je nach verwendetem Betriebssystem.
- 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 [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
- 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 [Verlassen der Amazon SES - Sandbox \(p. 79\)](#).

Konfigurieren von Postfix

Führen Sie die folgenden Verfahren durch, um Ihren E-Mail-Server für das Senden von E-Mails 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 = encrypt" \  
"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` im obigen Befehl mit dem SMTP-Endpunkt der gewünschten Region. Weitere Informationen finden Sie unter [Regionen \(p. 494\)](#).

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 Sie die Datei und schließen Sie sie.

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` mit dem entsprechenden SMTP-Benutzernamen und Passwort. Ihr SMTP-Benutzername und das Passwort unterscheiden sich von Ihrer AWS Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Weitere Informationen zu Anmeldeinformationen finden Sie unter [the section called "Abrufen Ihrer - SMTP-Anmeldeinformationen"](#) (p. 95).

Wenn Sie Amazon SES in einer anderen AWS Region als USA West (Oregon) verwenden, ersetzen Sie `email-smtp.us-west-2.amazonaws.com` im obigen Befehl mit dem SMTP-Endpunkt der gewünschten Region. Weitere Informationen finden Sie unter [Regionen](#) (p. 494).

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 > /etc/ssl/certs/ca-bundle.crt
```

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 `sender@example.com` durch Ihre Absender-E-Mail-Adresse. Die Absenderadresse muss für die Verwendung mit Amazon SES überprüft werden. Ersetzen Sie `recipient@example.com` durch die Zieladresse. 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](#) (p. 271) 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](#) (p. 551), 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="YVhZDFly2QzMGQ2N2U0YTZmODU"
```

```
--YVvhZDFly2QzMGQ2N2U0YTZmODU
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--
--YVvhZDFly2QzMGQ2N2U0YTZmODU
Content-Type: application/octet-stream
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="customers.txt"

SUQsRmlyc3ROYW11LExhc3ROYW11LENvdW50cnkKMzQ4LEpvaG4sU3RpbGVzLENh
bmFkYQo5MjM4OSxKaWUStGl1LENoaW5hCjczNCxTaGlybGV5LFJvZHZHJpZ3VleixV
bml0ZWQGU3RhdGVzCjI4OTMsQW5heWESX11bmdhcixJbmRpbYQ==
--YVvhZDFly2QzMGQ2N2U0YTZmODU--
```

Speichern Sie die Datei und schließen Sie sie.

3. Geben Sie in der Befehlszeile folgenden Befehl ein. Ersetzen Sie `sender@example.com` durch Ihre E-Mail-Adresse und `recipient@example.com` 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 mit 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 der folgenden Vorgehensweise in diesem Abschnitt erfahren Sie, wie Sie Sendmail so konfigurieren, dass E-Mails über Amazon SES gesendet werden. Dieses Verfahren wurde auf einem Server mit Ubuntu 18.04.2 LTS getestet.

Note

Sendmail ist eine Anwendung eines Drittanbieters 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.

Prerequisites

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 [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#)

Wenn Ihr Konto sich in der Amazon SES -Sandbox befindet, müssen Sie auch die Adressen verifizieren, an die Sie E-Mail-Nachrichten senden. Weitere Informationen finden Sie unter [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

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

- Wenn Sie Amazon SES verwenden, um E-Mails von einer Amazon EC2 Instance zu senden, müssen Sie möglicherweise eine Elastic IP-Adresse zu Ihrer Amazon EC2-Instance hinzufügen, damit empfangende E-Mail-Anbieter Ihre E-Mails annehmen. Weitere Informationen finden Sie unter [Amazon EC2 Elastic IP-Adressen](#) im Amazon EC2-Benutzerhandbuch für Linux-Instances.
- Standardmäßig beschränkt Amazon Elastic Compute Cloud (Amazon EC2) den E-Mail-Verkehr über Port 25. Um Zeitüberschreitungen beim Versenden 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 Einschränkung auf Port 25 von meiner Amazon EC2 Instance oder der AWS Lambda Funktion?](#) im AWS-Wissenszentrum.

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-Mails mit Amazon SES aus.

Important

Für das Verfahren in diesem Abschnitt wird davon ausgegangen, dass Sie Amazon SES in der AWS Region USA West (Oregon) einsetzen möchten. Wenn Sie eine andere Region verwenden möchten, ersetzen Sie alle Instances von `email-smtp.us-west-2.amazonaws.com` in diesem Verfahren mit dem SMTP-Endpunkt der gewünschten Region. Eine Liste der SMTP-Endpunkt-URLs für die AWS Regionen, in denen Amazon SES verfügbar ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen 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/authinfo` hinzu:

```
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:

- Ersetzen `email-smtp.us-west-2.amazonaws.com` Klicken Sie auf den Amazon SES S-SMTP-Endpunkt, den Sie verwenden möchten.
- Ersetzen `smtpUsername` durch Ihren Amazon SES SMTP-Benutzernamen.
- Ersetzen `smtpPassword` durch Ihr Amazon SES SMTP-Passwort.

Note

Ihr SMTP-Benutzername und das Passwort unterscheiden sich von Ihrer AWS Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Weitere Informationen zum Abrufen Ihres SMTP-Benutzernamens und Ihres Passworts finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen](#) (p. 95).

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 Befehl oben die `email-smtp.us-west-2.amazonaws.com` Mit der Adresse des -SMTP-Endpunkts von Amazon SES, den Sie verwenden möchten.

4. Geben Sie in der Befehlszeile den folgenden Befehl ein, um `/etc/mail/access.db` erneut 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 die folgenden Zeilen zur Datei `/etc/mail/sendmail.mc` vor allen `MAILER( )`-Definitionen hinzu.

```
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.

- Ersetzen `email-smtp.us-west-2.amazonaws.com` Sie mit dem -SMTP-Endpunkt von Amazon SES, den Sie verwenden möchten.
- Ersetzen Sie `example.com` durch die Domäne, über die Sie E-Mails senden möchten.

Wenn Sie fertig sind, speichern Sie die Datei.

Note

Amazon EC2 schränkt die Kommunikation standardmäßig über Port 25. Wenn Sie Sendmail in einer Amazon EC2 Instance verwenden, sollten Sie das [Request to Remove Email Sending Limitations \(Anforderung zum Entfernen von E-Mail-Sendebeschränkungen\)](#).

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
```

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
```

Ersetzen Sie `sender@example.com` durch Ihre Absender-E-Mail-Adresse. Ersetzen Sie `recipient@example.com` 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 oft unter `/var/log/mail.log` oder `/var/log/maillog`.

Integrieren von Amazon SES in IIS-SMTP-Server von Microsoft Windows

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 2012 auf einer Amazon EC2 Instance geschrieben. Sie können dieselbe Konfiguration auf Microsoft Windows Server 2008 und Microsoft Windows Server 2008 R2 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 zuerst Microsoft Windows Server 2012 ein. Sie verwenden dazu die folgenden Anweisungen.
 - a. Von der [Amazon EC2 Verwaltungskonsole](#) starten Sie eine neue Microsoft Windows Server 2012 Base Amazon EC2 Instance.
 - b. Connect zur Instance her und melden Sie sich mit Remote Desktop 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 6 Management Compatibility tools (eine Option unter dem Kontrollkästchen Web Server) hinzufügen.
 - 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) 6.0 Manager aus.
 - c. Klicken Sie mit der rechten Maustaste auf SMTP Virtual Server #1 und wählen Sie anschließend Properties aus.
 - d. Wählen Sie auf der Registerkarte Access unter Relay Restrictions die Option Relay aus.
 - e. Klicken Sie im Dialogfeld Relay Restrictions auf Add.
 - f. Geben Sie unter Single Computer 127.0.0.1 für die IP-Adresse ein. Sie haben diesem Server nun Zugriff für das Weiterleiten von E-Mails an Amazon SES über den IIS-SMTP-Service gewährt.

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 Single Computer 127.0.0.1 und Group of Computers 172.1.1.0 - 255.255.255.0 (im Bereich mit der Netzwerkmaske). Verwenden Sie für Connection Single Computer 127.0.0.1 und Group of Computers 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 aus.
 - b. Wählen Sie auf der Registerkarte Delivery die Option Outbound Security aus.
 - c. SelectStandardauthentifizierungGeben Sie dann Ihren Amazon SES SMTP-Benutzernamen und das Passwort ein. Sie können diese Anmeldeinformationen aus der Amazon SES Konsole mit dem Verfahren unter abrufen [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen](#) (p. 95).

Important

Ihr SMTP-Benutzername und das Passwort unterscheiden sich von Ihrer AWS-Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Verwenden Sie nicht Ihre AWS-Anmeldeinformationen für die Authentifizierung bei einem SMTP-Endpunkt. Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen](#) (p. 18).

- d. Stellen Sie sicher, dass TLS encryption ausgewählt ist.
- e. Kehren Sie zur Registerkarte Delivery zurück.
- f. Wählen Sie Outbound Connections aus.
- g. Stellen Sie im Dialogfeld Outbound Connections sicher, dass der Port 25 oder 587 ist.

Note

Wenn Ihr Mail-Server auf Amazon EC2 gehostet wird und Sie planen, E-Mails über Port 25 zu senden, müssen Sie zunächst die Port 25-Einschränkungen für Ihr Konto entfernen. Weitere Informationen finden Sie unter [Wie entferne ich die Einschränkung auf Port 25 von meiner Amazon EC2 Instance oder der AWS Lambda Funktion?](#) im AWS-Wissenszentrum.

- h. Wählen Sie Advanced (Erweitert) aus.
- i. Für dieIntelligente HostGeben Sie den Amazon SES Endpunkt ein, den Sie verwenden werden (zum Beispiemail-smtp.us-west-2.amazonaws.com) enthalten. Eine Liste der Endpunkt-URLs für die AWS Regionen, in denen Amazon SES verfügbar ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) imAllgemeine 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.

Integration von Amazon SES mit Exim

Exim ist ein Mail Transfer Agent (MTA), der äußerst flexibel und konfigurierbar ist. Weitere Informationen zu Exim finden Sie auf der [Exim-Website](#).

Note

Exim 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.

So konfigurieren Sie Exim für das Senden von E-Mails über Amazon SES

1. Öffnen Sie die Datei `/etc/exim.conf.local` in einem Texteditor. Wenn die Datei nicht vorhanden ist, kopieren Sie die Vorlage aus `/etc/exim4/exim4.conf.template`.

2. Nehmen Sie in `/etc/exim.conf.local` die folgenden Änderungen vor:

- a. Fügen Sie im Abschnitt `routers` nach der Zeile `begin routers` Folgendes hinzu:

```
send_via_ses:
driver = manualroute
domains = ! +local_domains
transport = ses_smtp
route_list = * email-smtp.us-west-2.amazonaws.com;
```

Ersetzen Sie im obigen Code `email-smtp.us-west-2.amazonaws.com` Verwenden Sie den SMTP-Endpunkt, den Sie zum Senden der Nachricht verwenden möchten. Weitere Informationen finden Sie unter [Regionen und Amazon SES \(p. 494\)](#).

- b. Fügen Sie im Abschnitt `transports` nach der Zeile `begin transports` Folgendes hinzu:

```
ses_smtp:
driver = smtp
port = 587
hosts_require_auth = *
hosts_require_tls = *
```

- c. Fügen Sie im Abschnitt `authenticators` nach der Zeile `begin authenticators` Folgendes hinzu:

```
ses_login:
driver = plaintext
public_name = LOGIN
client_send = : USERNAME : PASSWORD
```

Ersetzen Sie im vorherigen Code `USERNAME` durch Ihren SMTP-Benutzernamen und `PASSWORD` durch Ihr SMTP-Passwort.

Important

Ihre SMTP-Anmeldeinformationen sind nicht mit Ihrer AWS Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel identisch. Weitere Informationen zum Abrufen Ihrer SMTP-Anmeldeinformationen finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#).

3. Speichern `/etc/exim.conf.local`.
4. Wenn Sie die Aktualisierung der Konfiguration abgeschlossen haben, geben Sie den folgenden Befehl ein, um Exim neu zu starten.

```
sudo /etc/init.d/exim4 restart
```

Note

Dieser Befehl unterscheidet sich möglicherweise je nach verwendetem Betriebssystem.

5. Führen Sie in der Befehlszeile die folgenden Schritte aus, um eine Testnachricht zu senden:
- a. Geben Sie den folgenden Befehl ein:

```
exim -v recipient@example.com
```

Ersetzen Sie im vorherigen Befehl `recipient@example.com` durch die Adresse, an die Sie die Nachricht senden möchten.

- b. Geben Sie Folgendes ein und drücken Sie am Ende jeder Zeile Enter:


```
From: sender@example.com  
Subject: Test message  
This is a test.
```

Ersetzen Sie im voranstehenden Befehl *sender@example.com* durch die E-Mail-Adresse, von der Sie die Nachricht senden möchten.

Wenn Sie Enter nach dem letzten Zeitraum (.) drücken, beginnt Exim mit der Konversation mit dem SMTP-Server. Wenn die Verbindung nach dem Senden der Nachricht offen bleibt, drücken Sie Ctrl+D, um sie zu schließen.

Tip

Wenn die Nachricht nicht übermittelt wird, überprüfen Sie das E-Mail-Protokoll Ihres Systems auf Fehler. Das Exim-E-Mail-Protokoll befindet sich in der Regel unter `/var/log/exim4/mainlog`.

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

Sie können mit der SMTP-Schnittstelle von Amazon SES über die Befehlszeile Ihres Betriebssystems interagieren. Die in diesem Abschnitt beschriebenen Methoden dienen dazu, Ihre Verbindung zum SMTP-Endpunkt von Amazon SES 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 [Amazon SES SMTP-Probleme](#) (p. 518).

Prerequisites

Wenn Sie eine Verbindung mit der SMTP-Schnittstelle von Amazon SES herstellen, müssen Sie einen Satz von SMTP-Anmeldeinformationen angeben. Ihre SMTP-Anmeldeinformationen sind nicht mit den AWS Standard-Anmeldeinformationen identisch. 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"](#) (p. 95).

Testen Ihrer Verbindung mit der Amazon SES SMTP-Schnittstelle

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.

Dieser Abschnitt enthält Verfahren zum Testen der Verbindungen, sowohl mit OpenSSL (das in den meisten Linux-, macOS- und Unix-Distributionen enthalten ist und auch für Windows erhältlich 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 Befehl oben die *email-smtp.us-west-2.amazonaws.com* Verwenden Sie die URL des Amazon SES P-Endpunkt für Ihre AWS Region. Weitere Informationen finden Sie unter [Regionen \(p. 494\)](#).

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 Befehl oben die *email-smtp.us-west-2.amazonaws.com* Verwenden Sie die URL des Amazon SES P-Endpunkt für Ihre AWS Region. Weitere Informationen finden Sie unter [Regionen \(p. 494\)](#).

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-VCSDP1YZ
A1b2C3d4E5f6G7h8I9j0
```

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

PowerShell

Sie können die Berechtigung [Test-Netzverbindung](#) in PowerShell verwenden, um eine Verbindung mit dem Amazon SES SMTP-Server herzustellen.

Note

Die `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 das Verfahren in [Verwenden der Befehlszeile zum Senden von E-Mails mithilfe der Amazon SES -SMTP-Schnittstelle](#) (p. 115) ausführen, um eine Test-E-Mail-Nachricht zu senden.

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

- Geben Sie in PowerShell den folgenden Befehl ein, um eine Verbindung mit dem Amazon SES SMTP-Server herzustellen:

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

Ersetzen Sie im Befehl oben die `email-smtp.us-west-2.amazonaws.com` durch die URL Amazon SES SMTP-Endpunkts für Ihre AWS Region und ersetzen Sie `587` mit der Portnummer. Weitere Informationen zu regionalen Endpunkten in Amazon SES finden Sie unter [Regionen](#) (p. 494).

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

- Geben Sie den folgenden Befehl in die Befehlszeile ein, um Ihren SMTP-Benutzernamen zu kodieren. Geben Sie dabei anstelle von `SMTPUsername` Ihren SMTP-Benutzernamen ein:

```
echo -n "SMTPUsername" | openssl enc -base64
```

Notieren Sie sich die Ausgabe dieses Befehls.

2. Geben Sie den folgenden Befehl in die Befehlszeile ein, um Ihr SMTP-Passwort zu kodieren. Geben Sie dabei anstelle von `SMTPPassword` Ihr SMTP-Passwort ein:

```
echo -n "SMTPPassword" | openssl enc -base64
```

Notieren Sie sich die Ausgabe dieses Befehls.

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

```
EHLO example.com
AUTH LOGIN
Base64EncodedSMTPUserName
Base64EncodedSMTPPassword
MAIL FROM: sender@example.com
RCPT TO: recipient@example.com
DATA
X-SES-CONFIGURATION-SET: ConfigSet
From: Sender Name <sender@example.com>
To: recipient@example.com
Subject: Amazon SES SMTP Test

This message was sent using the Amazon SES SMTP interface.
.
QUIT
```

4. Nehmen Sie die folgenden Änderungen an der im vorherigen Schritt erstellten Datei vor:
 - Ersetzen Sie `example.com` durch Ihre sendende Domäne.
 - Ersetzen Sie `Base64EncodedSMTPUserName` durch Ihren base64-kodierten SMTP-Benutzernamen.
 - Ersetzen Sie `Base64EncodedSMTPPassword` durch Ihr base64-kodiertes SMTP-Passwort.
 - Ersetzen Sie `sender@example.com` durch die E-Mail-Adresse, von der aus Sie senden. Diese Identität muss verifiziert werden.
 - Ersetzen Sie `recipient@example.com` durch die E-Mail-Zieladresse. Wenn sich Ihr Amazon SES Konto noch in der Sandbox befindet, muss diese Adresse verifiziert werden.
 - Ersetzen Sie `ConfigSet` durch den Namen des [Konfigurationssatzes](#) (p. 271), den Sie beim Senden dieser E-Mail verwenden möchten.

Note

Wenn Sie keinen Konfigurationssatz verwenden möchten, können Sie die gesamte Zeile weglassen, die mit `X-SES-CONFIGURATION-SET` beginnt.

Wenn Sie fertig sind, speichern Sie die Datei unter `input.txt`.

5. Wählen Sie an der Befehlszeile eine der folgenden Optionen aus:
 - So senden Sie mithilfe von explizitem SSL über Port 587— Geben Sie den folgenden Befehl ein:

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

- So senden Sie mithilfe von implizitem SSL über Port 465— Geben Sie den folgenden Befehl ein:

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

Note

Ersetzen **email-smtp.us-west-2.amazonaws.com** Verwenden Sie die URL des Amazon SES P-Endpunkt für Ihre AWS Region. Weitere Informationen finden Sie unter [Regionen \(p. 494\)](#).

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

```
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 die [Net.mail.SmtpClient](#)-Klasse verwenden, um E-Mail-Nachrichten mit explizitem SSL über Port 587 zu senden.

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.

So senden Sie eine E-Mail-Nachricht über PowerShell mit explizitem SSL:

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:
 - Ersetzen Sie `sender@example.com` durch die E-Mail-Adresse, von der Sie die Nachricht senden möchten.
 - Ersetzen Sie `recipient@example.com` durch die Adresse, an die Sie die Nachricht senden möchten.
 - Ersetzen `email-smtp.us-west-2.amazonaws.com` durch die URL des Amazon SES P-Endpunkt für Ihre AWS Region. Weitere Informationen finden Sie unter [Regionen und Amazon SES \(p. 494\)](#).
3. Geben Sie in PowerShell den folgenden Befehl ein:

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

Ersetzen Sie 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 die [System.Web.Mail.SmtpMail](#)-Klasse verwenden, um E-Mail-Nachrichten mit implizitem SSL über Port 465 zu senden.

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.

So senden Sie eine E-Mail-Nachricht über PowerShell mit implizitem SSL:

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:
 - Ersetzen Sie `sender@example.com` durch die E-Mail-Adresse, von der Sie die Nachricht senden möchten.
 - Ersetzen Sie `recipient@example.com` durch die Adresse, an die Sie die Nachricht senden möchten.
 - Ersetzen `email-smtp.us-west-2.amazonaws.com` durch die URL des Amazon SES P-Endpunkts für Ihre AWS Region. Weitere Informationen finden Sie unter [Regionen und Amazon SES](#) (p. 494) .
3. Geben Sie in PowerShell den folgenden Befehl ein:

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

Ersetzen Sie 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 S-API verwenden, um Produktions-E-Mails über Amazon SES zu senden. Weitere Informationen über die SMTP-Schnittstelle finden Sie unter [Senden von E-Mails über die Amazon SES SMTP-Schnittstelle \(p. 94\)](#). In diesem Abschnitt wird beschrieben, wie Sie mithilfe der API E-Mails senden.

Sie können die Amazon SES API auch verwenden, um E-Mails zu 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 unter [Amazon Simple Email Service API-Referenz](#). Eine Liste der Endpunkt-URLs für die AWS Regionen, in denen Amazon SES verfügbar ist, finden Sie unter [Amazon Simple Email Service-Endpunkte und -kontingente](#) im Allgemeinen AWS-Referenz.

Sie können die API wie folgt aufrufen:

- Stellen Sie direkte HTTPS-Anfragen —Dies ist die fortschrittlichste Methode, da Sie die Authentifizierung und das Signieren Ihrer Anfragen manuell bearbeiten und die Anforderungen dann manuell erstellen müssen. Weitere Informationen zum Stellen von Anforderungen finden Sie unter [Verwenden der Amazon SES API \(p. 442\)](#).
- Verwenden Sie ein AWS S-SDK—Verwenden von AWS S-SDKs vereinfachen den Zugriff auf die APIs für mehrere AWS -Services, 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 -BefehlszeilenschnittstelleDie [AWS Command Line Interface](#) Amazon ist das Befehlszeilen-Tool für Amazon SES. Wir bieten auch das [AWS Tools for Windows PowerShell](#) für diejenigen an, die das Skript in der PowerShell-Umgebung erstellen.

Unabhängig davon, ob Sie direkt oder indirekt über ein AWS S-SDK auf die Amazon SES -API zugreifen, ist die [AWS Command Line Interface](#) oder die [AWS Tools for Windows PowerShell](#) bietet die Amazon SES -API zwei verschiedene Möglichkeiten zum Senden einer E-Mail, je nachdem, wie viel Kontrolle Sie über das Verfassen der E-Mail-Nachricht möchten:

- **Formatiert** —Amazon SES verfasst und sendet eine ordnungsgemäß formatierte E-Mail-Nachricht. Sie brauchen nur „Von:“ und „An:“ -Adressen, einen Betreff und den Text. Amazon SES übernimmt den Rest. Weitere Informationen finden Sie unter [Senden von formatierten E-Mails mithilfe der Amazon SES API \(p. 121\)](#).
- **Raw...** 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 Raw-E-Mails mithilfe der Amazon SES API \(p. 121\)](#).

Themen in diesem Abschnitt:

- [Senden von formatierten E-Mails mithilfe der Amazon SES API \(p. 121\)](#)
- [Senden von Raw-E-Mails mithilfe der Amazon SES API \(p. 121\)](#)

Senden von formatierten E-Mails mithilfe der Amazon SES API

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

Die Amazon SES API stellt die `SendEmail`. Sie können eine formatierte E-Mail erstellen und senden. `SendEmail` Für sind eine Absender- sowie eine Empfängeradresse, ein Betreff und ein Text (Text, HTML oder beides) der Nachricht erforderlich. Eine vollständige Beschreibung von `SendEmail` Wechseln Sie zu [Amazon Simple Email Service API-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](#).

Ein Beispiel für die Erstellung einer formatierten Nachricht mit dem AWS SDK for Java; oder dem AWS SDK for .NET finden Sie unter [Senden einer E-Mail mit dem AWS SDK for Java \(p. 38\)](#) bzw. [Senden einer E-Mail mit dem AWS SDK for .NET \(p. 35\)](#).

Tipps zur Erhöhung der E-Mail-Sendegeschwindigkeit bei mehreren `SendEmail`-Aufrufen finden Sie unter [Erhöhen des Durchsatzes mit Amazon SES \(p. 517\)](#).

Senden von Raw-E-Mails mithilfe der Amazon SES API

Sie können die Amazon SES `SendRawEmail`. So senden Sie hochgradig angepasste Nachrichten an die Empfänger.

Dieser Abschnitt enthält Verfahren zum Erstellen und Senden von Raw-E-Mails mit der Amazon SES -API.

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 \(p. 16\)](#).

Verwenden von MIME

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.

Die 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 enthält. 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. Sie enthält auch eine Anlage.

```
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

SUQsRmlyc3ROYW11LEExhc3ROYW11LENvdW50cnkKMzQ4LEpvaG4sU3RpbGVzLENhbmFkYQo5MjM4
OSxKaWUsTG11LENoaW5hCjczNCxTaGlybGV5LFJvZHZJpZ3VleixVbml0ZWQgU3RhdGVzCjI4OTMs
QW5heWEsSX11bmdhcixJbmRpyQ==

--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.

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

Um eine E-Mail-Adresse zu codieren, die im Umschlag der Nachricht verwendet wird, verwenden Sie Punycode-Codierung.

Um z. B. eine E-Mail an 张伟@example.com zu senden, verwenden Sie im lokalen Teil der Adresse (der Teil vor dem @-Zeichen) Punycode-Codierung. Die resultierende codierte Adresse lautet xn--cpqy30b@example.com.

Note

Diese Regel gilt nur für E-Mail-Adressen, die Sie im Umschlag der Nachricht angeben, nicht für die Nachrichten-Header. Wenn Sie die `SendRawEmail`-API verwenden, definieren die von Ihnen in den Parametern `Source` und `Destinations` angegebenen Adressen den Sender bzw. die Empfänger des Umschlags.

Weitere Informationen zur Punycode-Codierung finden Sie unter [RFC 3492](#).

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.

Wenn Sie beispielsweise die Zeichenfolge verwenden möchten „Як ти поживаєш?“ 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/0L7QtC40LLQsNGU0Yg/?=
```

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 सर्वप्रथम @ च्निह का चयन किया और इनही को ईमेल का आवधिकारक 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/4KSC4KS44KSsoIOckqOC1  
hyDgpKrgpLNgpLLgpL4g4KSILeCkruClh+CksidgpLjgpILgpKbgpYfgpLYg4KSt4KWH4KSc4KS+  
IHwg4KS4KWHIOckn+ClieCkruCksuCkv+CkguCKuOCkqCDgpKjgpYcg4KS54KWAIOckuOCksOC1  
jeCkteCkquCljeCksOCKpeCkriBAIOckmuCkv+CkqOC1jeCkuSDgpJXgpL4g4KSa4KSv4KSsoIOck  
leCkv+Ckr+CkviDgpJTgpLAg4KSH4KSo4KWN4KS54KWAIOckleCliyDgpIjgpK7gpYfgpLIg4KSV  
4KS+IOckhuCkteCkv+Ckt+CljeCkleCkvuCKsOCklSDgpK7gpL7gpKjgpL4g4KSc4KS+4KS4KS+  
IOckueCliAo=
```

Note

In einigen Fällen können Sie das 8-Bit verwenden `Content-Transfer-Encoding` in Nachrichten, die Sie mit Amazon SES senden. Wenn Amazon SES jedoch Änderungen an Ihren Nachrichten vornehmen muss (wenn Sie z. B. [Nachverfolgung öffnen und klicken](#) (p. 549)), wird der 8-Bit-codierte Inhalt möglicherweise nicht ordnungsgemäß angezeigt, wenn er in den Postfächern 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:

- Content-Type: 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"`
- Content-Disposition: Gibt an, wie der E-Mail-Client des Empfängers die Inhalte anordnen soll. Für Anlagen ist dieser Wert `Content-Disposition: attachment`.
- Content-Transfer-Encoding: Das Schema, das zum Codieren der Anlage verwendet wurde. Für Dateianlagen ist dieser Wert fast immer `base64`.

Amazon SES akzeptiert die gängigsten Dateitypen. Eine Liste der Dateitypen, die Amazon SES nicht akzeptiert, finden Sie unter [Nicht-unterstützte Anhangtypen](#) (p. 556).

Senden von Raw-E-Mails mithilfe der Amazon SES API

Die Amazon SES API stellt die `SendRawEmail` mit dieser Option können Sie eine E-Mail-Nachricht im angegebenen Format verfassen und senden. Eine vollständige Beschreibung von `SendRawEmail` finden Sie unter der [Amazon Simple Email Service API-Referenz](#).

Note

Tipps zur Erhöhung der E-Mail-Sendegeschwindigkeit bei mehreren `SendRawEmail`-Aufrufen finden Sie unter [Erhöhen des Durchsatzes mit Amazon SES](#) (p. 517).

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

Java

Das folgende Codebeispiel veranschaulicht, wie Sie mit der [JavaMail](#)-Bibliothek und dem [AWS SDK for Java](#) eine Raw-E-Mail erstellen und senden können.

```
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 for 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 for Python \(Boto\)](#) eine Raw-E-Mail erstellen und senden können.

```
import os
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

# 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 = "Customer service contact info"

# The full path to the file that will be attached to the email.
ATTACHMENT = "path/to/customers-to-contact.xlsx"
```

```
# The email body for recipients with non-HTML email clients.
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></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"

# Create a new SES resource and specify a region.
client = boto3.client('ses',region_name=AWS_REGION)

# Create a multipart/mixed parent container.
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)

# Add the attachment to the parent container.
msg.attach(att)
#print(msg)
try:
    #Provide the contents of the email.
    response = client.send_raw_email(
        Source=SENDER,
        Destinations=[
            RECIPIENT
        ],
        RawMessage={
            'Data':msg.as_string(),
        },
    ),
```



```
        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'])
```

So senden Sie personalisierte E-Mails über die Amazon SES-API aus

Sie können die Berechtigung [CreateTemplate](#)-Vorgang zum Erstellen von E-Mail-Vorlagen. Diese Vorlagen enthalten eine Betreffzeile und die Text- und HTML-Teile des E-Mail-Textes. Die Betreff- und Textabschnitte können auch eindeutige Werte enthalten, die für jeden Empfänger persönlich angepasst sind.

Es gibt einige Beschränkungen und andere Überlegungen bei der Verwendung dieser Funktionen:

- Sie können bis zu 10.000 E-Mail-Vorlagen pro Amazon SES Konto erstellen.
- Jede Vorlage kann bis zu 500 KB groß sein, einschließlich Text- und HTML-Teile.
- Sie können eine unbegrenzte Anzahl an Ersetzungsvariablen in jede Vorlage einschließen.
- Sie können bei jedem Aufruf der `SendBulkTemplatedEmail`-Operation E-Mails an bis zu 50 Zieladressen senden. Eine Zieladresse umfasst eine Liste der Empfänger sowie CC- und BCC-Empfänger. Beachten Sie, dass die Anzahl der Zieladressen, die Sie in einem einzigen Aufruf der API kontaktieren können, auf die maximale Senderate Ihres Kontos beschränkt sein kann. Weitere Informationen finden Sie unter [Verwalten Ihrer Amazon SES Versandkontingente \(p. 156\)](#).

Dieser Abschnitt enthält Verfahren zum Erstellen von E-Mail-Vorlagen und zum Senden von personalisierten E-Mails.

Note

Bei den Verfahren in diesem Abschnitt wird davon ausgegangen, dass Sie die bereits installiert und konfiguriert haben AWS CLI. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

Teil 1 Ereignisbenachrichtigungen für Rendering-Fehler

Wenn Sie eine E-Mail versenden, die ungültige Personalisierungsinhalte enthält, akzeptiert Amazon SES die Nachricht möglicherweise, kann sie jedoch nicht zustellen. Wenn Sie vorhaben, eine personalisierte E-Mail zu versenden, sollten Sie aus diesem Grund Amazon SES so konfigurieren, dass über Amazon SNS Benachrichtigungen über Rendering-Fehlerereignisse 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. Die entsprechenden Verfahren sind 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.

Die entsprechenden Verfahren sind unter beschrieben. [Abonnieren eines Themas](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

3. Schließen Sie die Verfahren in [the section called "Einrichten eines Amazon SNS-Ziels"](#) (p. 322) So richten Sie Ihre Konfigurationssätze ein, um Rendering-Fehlerereignisse in Ihrem Amazon SNS - Thema zu erstellen.

Teil 2: Erstellen einer E-Mail-Vorlage

In diesem Abschnitt verwenden Sie die API-Operation `CreateTemplate`, um eine neue E-Mail-Vorlage mit Personalisierungsattributen zu erstellen.

Bei diesem Verfahren wird vorausgesetzt, dass Sie die AWS CLI bereits installiert und konfiguriert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So erstellen Sie die Vorlage

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

```
{
  "Template": {
    "TemplateName": "MyTemplate",
    "SubjectPart": "Greetings, {{name}}!",
    "HtmlPart": "<h1>Hello {{name}},</h1><p>Your favorite animal is  
{{favoriteanimal}}.</p>",
    "TextPart": "Dear {{name}},\r\nYour favorite animal is {{favoriteanimal}}."
  }
}
```

Dieser Code enthält die folgenden Eigenschaften:

- **TemplateName**— Der Name der Vorlage. Beim Senden der E-Mail-Adresse beziehen Sie sich auf diesen Namen.
- **SubjectPart**— Die Betreffzeile der E-Mail. Diese Eigenschaft kann Ersatz-Tags enthalten. Diese Tags weisen das folgende Format auf: `{{tagname}}`. Wenn Sie die E-Mail senden, können Sie einen Wert für `tagname` für jedes Ziel.

Das vorherige Beispiel umfasst zwei Tags: `{{name}}` und `{{favoriteanimal}}`.

- **HtmlPart**— Der HTML-Text der E-Mail. Diese Eigenschaft kann Ersatz-Tags enthalten.
 - **TextPart**— Der Textkörper der E-Mail. Empfänger, deren E-Mail-Clients keine HTML-E-Mails anzeigen, sehen diese Version der E-Mail. Diese Eigenschaft kann 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 an der Befehlszeile den folgenden Befehl ein, um mithilfe der eine neue Vorlage zu erstellen `CreateTemplate` API-Operation:

```
aws ses create-template --cli-input-json file://mytemplate.json
```

Teil 3: Senden der personalisierten E-Mail

Nach dem Erstellen einer E-Mail-Vorlage können Sie mit ihr eine E-Mail senden. Es gibt zwei API-Operationen, die Sie verwenden können, um E-Mails mit Vorlagen zu senden: `SendTemplatedEmail` und `SendBulkTemplatedEmail`. Die `SendTemplatedEmail`-Operation ist hilfreich für das Senden

einer angepassten E-Mail an eine einzelne Zieladresse (eine Sammlung von "To"-, "CC"- und "BCC"-Empfängern, die dieselbe E-Mail erhalten). Die `SendBulkTemplatedEmail`-Operation lässt sich eindeutige E-Mails an mehrere Zieladressen in einem einzigen Aufruf der Amazon SES -API senden. Dieser Abschnitt zeigt Beispiele, wie die AWS CLI zum Senden von E-Mail mithilfe dieser beiden Operationen verwendet wird.

Senden von E-Mail-Vorlagen an eine einzelne Zieladresse

Verwenden Sie die `SendTemplatedEmail`-Operation, um eine E-Mail an eine einzelne Zieladresse zu senden. Alle Empfänger im `Destination`-Objekt erhalten dieselbe E-Mail.

So senden Sie eine E-Mail-Vorlage an eine einzelne Zieladresse

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

```
{
  "Source": "Mary Major <mary.major@example.com>",
  "Template": "MyTemplate",
  "ConfigurationSetName": "ConfigSet",
  "Destination": {
    "ToAddresses": [ "alejandro.rosalez@example.com" ]
  },
  "TemplateData": "{ \"name\": \"Alejandro\", \"favoriteanimal\": \"alligator\" }"
}
```

Dieser Code enthält die folgenden Eigenschaften:

- Source – Die E-Mail-Adresse des Absenders.
- Template – Der Name der Vorlage, die auf die E-Mail angewendet werden soll.
- ConfigurationSetName – der Name des Konfigurationssatzes, der beim Senden der E-Mail verwendet wird.

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 “Teil 1: Einrichten von Benachrichtigungen” \(p. 129\)](#).

- Zielbereich— Die Empfängeradressen. Sie können mehrere "To"-, "CC"- und "BCC"-Adressen einschließen. Wenn Sie die `SendTemplatedEmail`-Operation verwenden, erhalten alle Empfänger die gleiche E-Mail.
 - TemplateData— Eine Escape-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.
2. Ändern Sie die Werte im obigen Code Ihren Bedürfnissen entsprechend ab, und speichern Sie die Datei anschließend unter `myemail.json`.
 3. Geben Sie den folgenden Befehl in der Befehlszeile ein, um die E-Mail zu senden:

```
aws ses send-templated-email --cli-input-json file://myemail.json
```

Senden von E-Mail-Vorlagen an mehrere Zieladressen

Sie können die `BerechtigungSendBulkTemplatedEmail`-Operation, um eine E-Mail an mehrere Zieladressen in einem einzigen Aufruf der API zu senden. Jeder Empfänger von Amazon SES sendet eine eindeutige E-Mail an den bzw. die Empfänger in jedem `Destination`-Objekt.

So senden Sie eine E-Mail-Vorlage an mehrere Zieladressen

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

```
{
  "Source": "Mary Major <mary.major@example.com>",
  "Template": "MyTemplate",
  "ConfigurationSetName": "ConfigSet",
  "Destinations": [
    {
      "Destination": {
        "ToAddresses": [
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementTemplateData": "{ \"name\": \"Anaya\", \"favoriteanimal\": \"angelfish\" }"
    },
    {
      "Destination": {
        "ToAddresses": [
          "liu.jie@example.com"
        ]
      },
      "ReplacementTemplateData": "{ \"name\": \"Liu\", \"favoriteanimal\": \"lion\" }"
    },
    {
      "Destination": {
        "ToAddresses": [
          "shirley.rodriquez@example.com"
        ]
      },
      "ReplacementTemplateData": "{ \"name\": \"Shirley\", \"favoriteanimal\": \"shark\" }"
    },
    {
      "Destination": {
        "ToAddresses": [
          "richard.roe@example.com"
        ]
      },
      "ReplacementTemplateData": "{}"
    }
  ],
  "DefaultTemplateData": "{ \"name\": \"friend\", \"favoriteanimal\": \"unknown\" }"
}
```

Dieser Code enthält die folgenden Eigenschaften:

- Source – Die E-Mail-Adresse des Absenders.
- Template – Der Name der Vorlage, die auf die E-Mail angewendet werden soll.
- ConfigurationSetName – der Name des Konfigurationssatzes, der beim Senden der E-Mail verwendet wird.

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 “Teil 1: Einrichten von Benachrichtigungen” \(p. 129\)](#).

- Destinations – Ein Array mit einer oder mehreren Zieladressen.

- **Zielbereich**— Die Empfängeradressen. Sie können mehrere "To"-, "CC"- und "BCC"-Adressen einschließen. Wenn Sie die `SendBulkTemplatedEmail`-Operation verwenden, erhalten alle Empfänger innerhalb desselben `Destination`-Objekts die gleiche E-Mail.
 - **ReplacementTemplateData**— Ein JSON-Objekt mit Schlüssel-Wert-Paaren. 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.
 - **DefaultTemplateData**— Ein JSON-Objekt mit Schlüssel-Wert-Paaren. 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. Das Objekt enthält Fallback-Daten. Wenn ein `Destination`-Objekt ein leeres JSON-Objekt in der `ReplacementTemplateData`-Eigenschaft enthält, werden die Werte in der `DefaultTemplateData`-Eigenschaft verwendet.
2. Ändern Sie die Werte im obigen Code Ihren Bedürfnissen entsprechend ab, und speichern Sie die Datei anschließend unter `mybulkemail.json`.
 3. Geben Sie den folgenden Befehl in der Befehlszeile ein, um die Massen-E-Mail zu senden:

```
aws ses send-bulk-templated-email --cli-input-json file://mybulkemail.json
```

Erweiterte E-Mail-Personalisierung

Die Vorlagenfunktion in Amazon SES basiert auf dem Handlebars-Vorlagensystem. Verwenden Sie Handlebars, um Vorlagen mit erweiterten Funktionen wie verschachtelten Attributen, Array-Iteration, grundlegenden bedingten Anweisungen und dem Erstellen von eingebetteten Teilen zu erstellen. 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.

Themen

- [Analysieren von verschachtelten Attributen](#) (p. 133)
- [Durchlaufen von Listen](#) (p. 134)
- [Verwenden von grundlegenden bedingten Anweisungen](#) (p. 135)
- [Erstellen von eingebundene Teilen](#) (p. 137)

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/preferences/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/preferences/i.aspx?id={{meta.userId}}"
  }
}
```

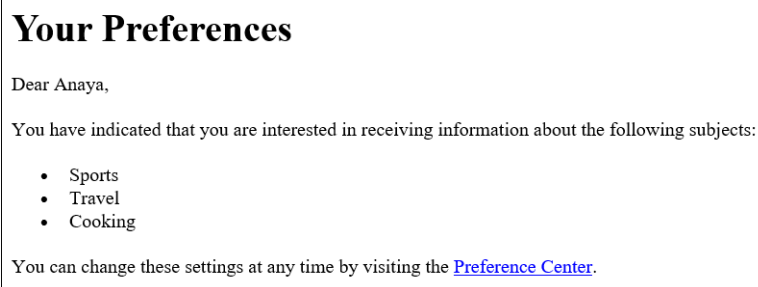
Important

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 `SendTemplatedEmail` oder `SendBulkTemplatedEmail` 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\"}]}"
    },
    {
      "Destination": {
        "ToAddresses": [
          "friend@example.com"
        ]
      },
      "ReplacementTemplateData": "{\"meta\":{\"userId\":\"\"},\"contact\":{\"firstName\":\"Friend\",\"lastName\":\"\"},\"subscription\":[]}"
    }
  ],
  "DefaultTemplateData": "{\"meta\":{\"userId\":\"\"},\"contact\":{\"firstName\":\"Friend\",\"lastName\":\"\"},\"subscription\":[]}"
}
```

Wenn Sie mithilfe der Operation `SendBulkTemplatedEmail` eine E-Mail an die Empfänger aus dem vorherigen Beispiel senden, erhalten diese eine Nachricht ähnlich wie in der folgenden Abbildung:



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/preferences/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/preferences/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/preferences/i.aspx?
id={{meta.userId}}.
  {{else}}
  Please update your subscription preferences by visiting the
Preference Center at https://www.example.com/preferences/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:

Your Preferences

Dear Shirley,

Please update your subscription preferences by visiting the [Preference Center](#).

Erstellen von eingebundene Teilen

Mithilfe von eingebetteten Teilen können Sie Vorlagen vereinfachen, die wiederholte Zeichenfolgen enthalten. Sie können beispielsweise 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 die `fullName` als Teil können Sie ihn an jeder Stelle in Ihrer Vorlage einfügen, 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 Empfängeramen 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.

Verwalten von E-Mail-Vorlagen

Zusätzlich zu [Erstellen von E-Mail-Vorlagen](#) (p. 129) können Sie die Amazon SES API auch verwenden, um vorhandene Vorlagen zu aktualisieren oder zu löschen, alle vorhandenen Vorlagen aufzulisten oder den Inhalt einer Vorlage anzuzeigen.

In diesem Abschnitt werden Verfahren für die Verwendung der AWS CLI, um Aufgaben im Zusammenhang mit Amazon SES Vorlagen auszuführen.

Note

Bei den Verfahren in diesem Abschnitt wird davon ausgegangen, dass Sie die bereits installiert und konfiguriert haben AWS CLI. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

Anzeigen einer Liste von E-Mail-Vorlagen

Sie können die Berechtigung `ListTemplates` in der Amazon SES -API verwenden, um eine Liste mit all Ihren vorhandenen E-Mail-Vorlagen anzuzeigen.

So zeigen Sie eine Liste von E-Mail-Vorlagen an

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses list-templates
```

Wenn in Ihrem Amazon 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 eine `TemplatesMetadata`-Objekt ohne Elemente.

Anzeigen des Inhalts einer bestimmten E-Mail-Vorlage

Sie können die Berechtigung `GetTemplate` in der Amazon SES API 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 ses get-template --template-name MyTemplate
```

Ersetzen Sie im Befehl oben die *MyTemplate* Klicken Sie auf den Namen der Vorlage, die Sie anzeigen möchten.

Wenn der von Ihnen angegebene Vorlagenname mit einer Vorlage übereinstimmt, die in Ihrem Amazon 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!\n</h2>\n<p>This is the HTML part of the  
message.\n</p>\n</body>\n</html>"  
  }  
}
```

Wenn der von Ihnen angegebene Vorlagenname nicht mit einer Vorlage übereinstimmt, die in Ihrem Amazon SES Konto vorhanden ist, gibt der Befehl eine `TemplateDoesNotExist`-Fehler.

Löschen einer E-Mail-Vorlage

Sie können die Berechtigung `DeleteTemplate`-Operation in der Amazon SES API verwenden, um eine bestimmte E-Mail-Vorlage zu löschen.

So löschen Sie eine E-Mail-Vorlage

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-template --template-name MyTemplate
```

Ersetzen Sie im Befehl oben den Befehl oben *MyTemplate* Klicken Sie auf den Namen der Vorlage, die Sie löschen möchten.

Mit diesem Befehl wird keine Ausgabe bereitgestellt. Ob die Vorlage gelöscht wurde, können Sie durch das Verwenden der `GetTemplate` (p. 139) verwenden.

Aktualisieren einer E-Mail-Vorlage

Sie können die Berechtigung [UpdateTemplate](#) verwenden, um einen Vorgang in der Amazon SES API, 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.

So aktualisieren Sie eine E-Mail-Vorlage

1. Verwenden der `GetTemplate` Rufen Sie die vorhandene Vorlage ab, indem Sie den folgenden Befehl in der Befehlszeile eingeben:

```
aws ses get-template --template-name MyTemplate
```

Ersetzen Sie im Befehl oben den Befehl oben *MyTemplate* durch den Namen der Vorlage, die Sie aktualisieren möchten.

Wenn der von Ihnen angegebene Vorlagenname mit einer Vorlage übereinstimmt, die in Ihrem Amazon 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>\n</body>\n</html>"
  }
}
```

2. Erstellen Sie in einem Texteditor eine neue Datei. Fügen Sie die Ausgabe des 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 die `SubjectPart` der Vorlage verwenden, müssen Sie weiterhin die `TextPart` und `HtmlPart`-Eigenschaften.

Wenn Sie fertig sind, speichern Sie die Datei unter `update_template.json`.

4. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses update-template --cli-input-json file://path/to/update_template.json
```

Ersetzen Sie im Befehl oben den Befehl oben *Pfad/zum/update_template.json* mit dem Pfad zum `update_template.json`. Die Datei, die Sie im vorherigen Schritt erstellt haben.

Wenn die Vorlage erfolgreich aktualisiert wurde, liefert dieser Befehl keine Ausgabe. Sie können überprüfen, ob die Vorlage aktualisiert wurde, indem Sie mithilfe der [GetTemplate](#) (p. 139) verwenden.

Wenn die von Ihnen angegebene Vorlage nicht vorhanden ist, gibt dieser Befehl eine `TemplateDoesNotExist`-Fehler. Wenn die Vorlage weder die `TextPart` oder `HtmlPart`-Eigenschaft (oder beides), gibt dieser Befehl eine `InvalidParameterValue`-Fehler.

Amazon Authentifizieren Ihrer E-Mails in Amazon SES

Amazon Simple Email Service (Amazon SES) nutzt zum Senden von E-Mails 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, die E-Mail-Verkehr weiterleiten, haben Schritte unternommen, um die Seriosität von E-Mails zu bewerten. Eine solche Maßnahme, die Internetdienstanbieter treffen, ist zu bestimmen, ob eine E-Mail authentifiziert wird. Für die Authentifizierung ist es erforderlich, dass Sender verifizieren, dass sie der Besitzer des sendenden Kontos sind. Mitunter verweigern Internetdienstanbieter die Weiterleitung von E-Mail, die nicht authentifiziert ist. Für optimale Zustellbarkeit empfehlen wir, dass Sie Ihre E-Mails authentifizieren.

In den folgenden Abschnitten werden zwei Authentifizierungsmechanismen beschrieben, die ISPs verwenden — Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) — und Anleitungen für die Verwendung dieser Standards mit Amazon SES bereitgestellt.

- 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 \(p. 141\)](#).
- Weitere Informationen zu DKIM, einem Standard, über den Sie Ihre E-Mails signieren können, um ISPs zu zeigen, dass Ihre Nachrichten legitim sind und während der Übertragung nicht geändert wurden, finden Sie unter [Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES \(p. 142\)](#).
- 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 von DMARC mit Amazon SES \(p. 154\)](#).

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.

Um SPF einzurichten, veröffentlichen Sie einen TXT-Datensatz in der DNS-Konfiguration für Ihre Domäne. Dieser Datensatz enthält eine Liste der Server, die Sie zum Senden von E-Mails aus Ihrer Domäne autorisieren. Wenn ein E-Mail-Anbieter eine Nachricht von Ihrer Domäne empfängt, überprüft er die DNS-Datensätze für Ihre Domäne darauf, ob die E-Mail von einem autorisierten Server gesendet wurde.

Wenn Sie E-Mails über Amazon SES senden, bestehen die von Ihnen gesendeten Nachrichten standardmäßig eine SPF-Prüfung. Amazon SES gibt eine MAIL FROM-Domäne für jede Nachricht an, die eine Subdomain vonamazonses.com und der sendende Mail-Server für die Nachricht wird mit dieser Domäne ausgerichtet.

Sie können optional Ihren eigenen SPF-Datensatz veröffentlichen. Durch die Veröffentlichung eines SPF-Datensatzes kann Ihre E-Mail mit Domain-based Message Authentication, Reporting and Conformance (DMARC) konform sein. Weitere Informationen finden Sie unter [Einhaltung von DMARC \(p. 154\)](#).

Hinzufügen eines SPF-Datensatzes

Um einen SPF-Datensatz zu veröffentlichen, müssen Sie einen neuen TXT-Datensatz zur DNS-Konfiguration für Ihre Domäne hinzufügen. Die Verfahren zum Aktualisieren von DNS-Datensätzen variieren je nachdem, welchen DNS- oder Webhosting-Anbieter Sie verwenden.

Links zur Dokumentation für mehrere gängige Anbieter werden in der nachfolgenden Tabelle aufgelistet. Diese Liste ist nicht vollständig und die Aufnahme in diese Liste ist keine Befürwortung oder Empfehlung für die Produkte oder Dienstleistungen eines Unternehmens. Wenn Ihr Anbieter nicht in der Tabelle aufgeführt ist, können Sie wahrscheinlich trotzdem einen SPF-Datensatz veröffentlichen.

DNS/Hosting-Anbieter	Link zur Dokumentation
Amazon Route 53	Erstellen von Datensätzen mithilfe der Amazon Route 53 Konsole
GoDaddy	Hinzufügen eines SPF-Datensatzes
Dreamhost	Wie füge ich einen SPF-Datensatz hinzu?
Cloudflare	Verwalten von DNS-Datensätzen in CloudFlare
HostGator	SPF-Datensätze
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC-Datensätze für meine Domain hinzu?
Names.co.uk	Ändern der DNS-Einstellungen Ihrer Domäne
Wix	Hinzufügen oder Aktualisieren von SPF-Datensätzen in Ihrem Wix-Konto

Wenn Ihre Domäne über keinen SPF-Datensatz verfügt, veröffentlichen Sie einen TXT-Eintrag mit dem folgenden Wert. Der Name des Datensatzes kann leer oder @ sein, abhängig von Ihrem DNS-Service.

```
"v=spf1 include:amazonses.com ~all"
```

SPF-Datensätze können mehrere `include`-Anweisungen enthalten. Wenn Ihre Domäne bereits über einen SPF-Eintrag verfügt, können Sie eine `include`-Anweisung für Amazon SES verwenden, indem Sie das folgende Format verwenden:

```
"v=spf1 include:example.com include:amazonses.com ~all"
```

Authentifizierung Ihrer E-Mails mit DKIM in Amazon SES

DomainKeys Identified Mail (DKIM) ist ein Standard, mit dem Versender ihre E-Mails mit einem kryptografischen Schlüssel signieren können. E-Mail-Anbieter können dann anhand dieser Signaturen sicherstellen, dass die Nachrichten nicht während der Übertragung von einem Dritten geändert wurden.

Eine E-Mail-Nachricht, die mit DKIM gesendet wird, enthält ein DKIM-Signatur-Header-Feld mit einer kryptografisch signierten Darstellung der Nachricht oder eines Teils davon. Ein Anbieter, der eine Nachricht empfängt, kann mit einem öffentlichen Schlüssel, der im DNS-Datensatz des Absenders veröffentlicht ist, die Signatur entschlüsseln. E-Mail-Anbieter ermitteln mit diesen Informationen dann, ob die E-Mail-Nachrichten echt sind.

DKIM-Signaturen sind optional. Sie können Ihre E-Mail mit einer DKIM-Signatur signieren, um die Zustellbarkeit mit DKIM-kompatiblen E-Mail-Anbietern zu verbessern. Amazon SES bietet drei Möglichkeiten zum Signieren von Nachrichten mit einer DKIM-Signatur:

- Informationen zum Einrichten einer Sender-ID (z. B. einer Domäne oder einer E-Mail-Adresse), damit Amazon SES automatisch eine DKIM-Signatur zu allen Nachrichten hinzufügt, die Sie über diese Identität versenden, erfahren Sie unter [Einfache DKIM in Amazon SES \(p. 143\)](#).
- Informationen zum Verwenden Ihres eigenen Schlüsselpaars aus öffentlichem und privatem Schlüssel für die DKIM-Authentifizierung finden Sie unter [Bereitstellen Ihres eigenen DKIM-Authentifizierungstokens in Amazon SES \(p. 150\)](#)

- Informationen zum Hinzufügen Ihrer eigenen DKIM-Signatur zu jeder E-Mail, die Sie mit der `SendRawEmail`-API senden, finden Sie unter [Manuelle DKIM-Signierung in Amazon SES \(p. 154\)](#).

Einfache DKIM in Amazon SES

Wenn Sie Easy DKIM für eine ID einrichten, fügt Amazon SES automatisch einen 1024-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.

Wenn Sie Easy DKIM erfolgreich konfigurieren, können Sie E-Mails von der DKIM-fähigen Domäne senden. Dies gilt auch, wenn Sie die in [Verifizieren einer Domäne mit Amazon SES \(p. 66\)](#) beschriebenen Vorgänge noch nicht abgeschlossen haben.

Überlegungen zu Easy DKIM

Wenn Sie Ihre E-Mails mit Easy DKIM authentifizieren, gelten die folgenden Regeln:

- Sie müssen Easy DKIM nur für die Domäne einrichten, die Sie bei Ihrer Absenderadresse verwenden. Sie müssen Easy DKIM nicht für Domänen einrichten, die Sie bei der "Return-Path"-Adresse oder der Antwortadresse verwenden.
- Amazon SES ist in verschiedenen AWS Regionen verfügbar. Wenn Sie mehr als eine AWS Region für das Senden von E-Mails verwenden, müssen Sie den Easy DKIM-Setup-Prozess in jeder dieser Regionen durchführen, um sicherzustellen, dass all Ihre E-Mails mit einer DKIM-Signatur versehen werden.
- Wenn Sie eine Domäne verifizieren, gelten Ihre Easy DKIM-Einstellungen auch für alle Subdomänen dieser Domäne, es sei denn, Sie richten Easy DKIM für bestimmte Subdomänen ein.
- Wenn Sie Easy DKIM für eine übergeordnete Domäne, eine Subdomäne und eine E-Mail-Adresse einrichten, wendet Amazon SES die Easy DKIM-Einstellungen wie folgt an:
 - DKIM-Einstellungen für eine Subdomäne überschreiben die Einstellungen für die übergeordnete Domäne.
 - DKIM-Einstellungen für eine E-Mail-Adresse überschreiben die Einstellungen für die Subdomäne (falls zutreffend) und die übergeordnete Domäne.

Dieses Thema enthält die folgenden Abschnitte:

- [Einrichten von Easy DKIM für eine Domäne \(p. 143\)](#)
- [Einrichten von Easy DKIM für eine E-Mail-Adresse \(p. 145\)](#)
- [Verwalten von Easy DKIM \(p. 146\)](#)

Einrichten von Easy DKIM für eine Domäne

Das Verfahren in diesem Abschnitt zeigt Ihnen, wie Sie Easy DKIM für eine Domäne einrichten. Wenn Sie Easy DKIM für eine Domäne einrichten, können Sie mit dem Senden von E-Mails von dieser Domäne beginnen, selbst wenn Sie das [Verfahren zum Überprüfen einer Domäne \(p. 65\)](#) noch nicht abgeschlossen haben.

So richten Sie Easy DKIM für eine Domäne ein

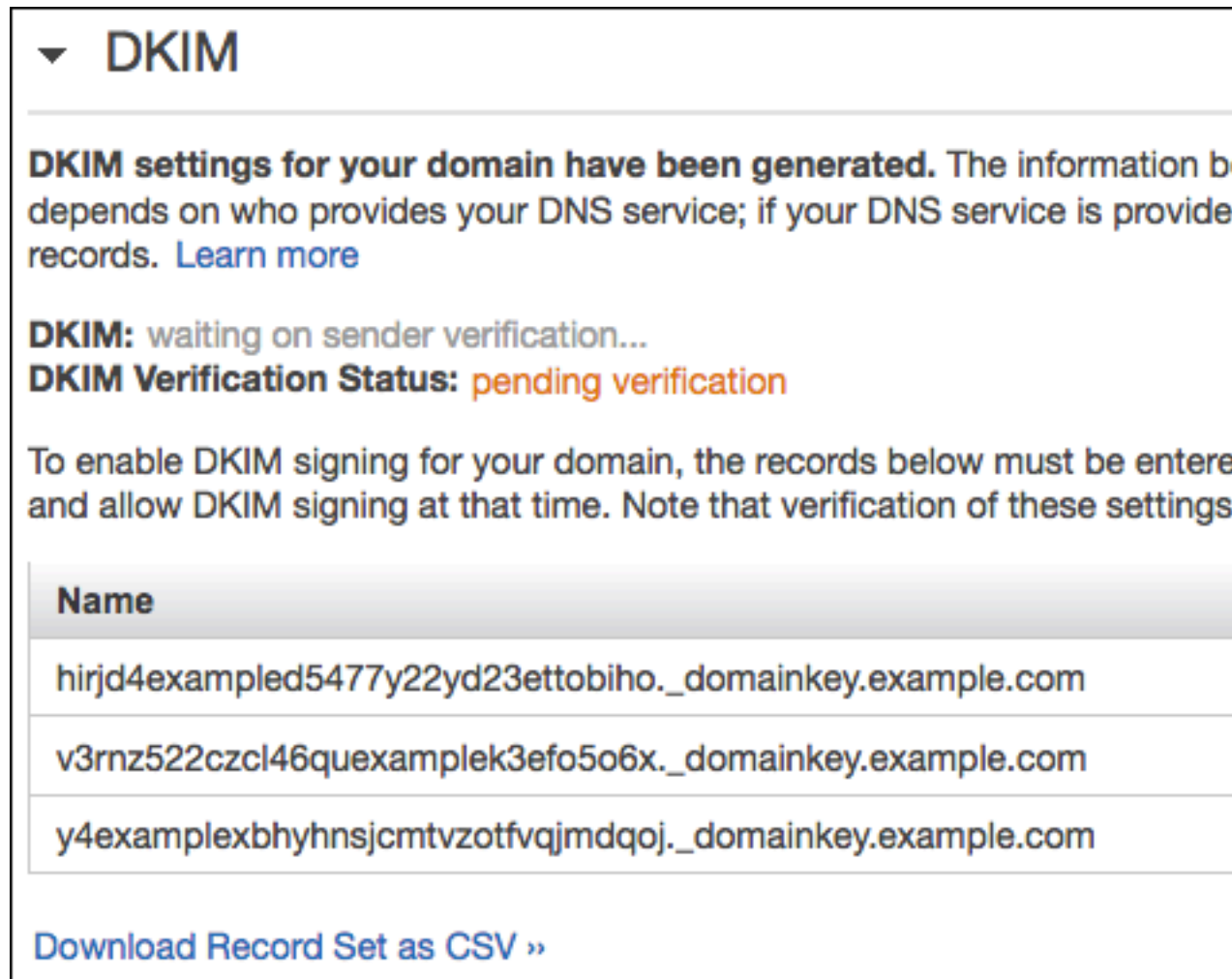
1. Öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management die Option Domains aus.
3. Wählen Sie aus der Liste der Domänen die Domäne aus, für die Sie Easy DKIM einrichten möchten.

Note

Wenn Sie den Verifizierungsprozess für die Domäne noch nicht gestartet haben, schlagen Sie die Verfahren unter [Verifizieren einer Domäne mit Amazon SES \(p. 66\)](#) nach.

4. Wählen Sie unter DKIM die Option Generate DKIM Settings (DKIM-Einstellungen generieren) aus.
5. Kopieren Sie die drei CNAME-Datensätze, 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 zeigt ein Beispiel für den Bereich DKIM.



▼ DKIM

DKIM settings for your domain have been generated. The information b depends on who provides your DNS service; if your DNS service is provide records. [Learn more](#)

DKIM: waiting on sender verification...

DKIM Verification Status: pending verification

To enable DKIM signing for your domain, the records below must be entered and allow DKIM signing at that time. Note that verification of these settings

Name
hirjd4exampled5477y22yd23ettobiho._domainkey.example.com
v3rnz522czcl46quexamplek3efo5o6x._domainkey.example.com
y4examplexbhyhnsjcmtvzotfvqjmdqoj._domainkey.example.com

[Download Record Set as CSV »](#)

6. Fügen Sie die CNAME-Datensätze zur DNS-Konfiguration für Ihre Domäne hinzu. So aktualisieren Sie die DNS-Datensätze für Ihre Domäne:
 - Wenn Sie Route 53 als DNS-Anbieter verwenden— Wenn Sie Route 53 für dasselbe Konto verwenden, das Sie beim Senden von E-Mails mit Amazon SES verwenden, wählen Sie Route 53

verwenden. So aktualisieren Sie die DNS-Einstellungen für Ihre Domäne automatisch. Andernfalls führen Sie die Verfahren unter [Bearbeiten von Datensätzen](#) im Amazon Route 53 Entwicklerhandbuch.

- Wenn Sie einen anderen DNS-Anbieter verwenden: Verschiedene Anbieter nutzen unterschiedliche Verfahren zum Aktualisieren von DNS-Datensätzen. Links zu der Dokumentation für mehrere gängige Anbieter werden in der nachfolgenden Tabelle aufgelistet. Diese Liste ist nicht vollständig und die Aufnahme in diese Liste ist keine Empfehlung oder Empfehlung für die Produkte oder Dienstleistungen eines Unternehmens. Wenn Ihr Anbieter in der Tabelle nicht aufgeführt ist, können Sie die Domäne wahrscheinlich mit Amazon SES verwenden.

DNS/Hosting-Anbieter	Link zur Dokumentation
GoDaddy	Hinzufügen eines CNAME-Datensatzes
Dreamhost	Wie füge ich benutzerdefinierte DNS-Datensätze hinzu?
Cloudflare	Wie füge ich einen CNAME-Datensatz hinzu?
HostGator	Verwalten von DNS-Datensätzen mit HostGator/eNOM
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC-Datensätze für meine Domain hinzu?
Names.co.uk	Ändern der DNS-Einstellungen Ihrer Domäne
Wix	Hinzufügen oder Aktualisieren von CNAME-Datensätzen in Ihrem Wix-Konto

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.

- Wenn Sie sich nicht sicher sind, wer Ihr DNS-Anbieter ist: Weitere Informationen erhalten Sie bei Ihrem Systemadministrator.

Amazon SES erkennt Änderungen an der DNS-Konfiguration in der Regel innerhalb von 72 Stunden.

Einrichten von Easy DKIM für eine E-Mail-Adresse

Die Verfahren in diesem Abschnitt zeigt Ihnen, wie Sie Easy DKIM für eine bestimmte E-Mail-Adresse einrichten, die Sie bereits mit Amazon SES überprüft haben. Sie können Easy DKIM nur für E-Mail-Adressen konfigurieren, die zu Domänen gehören, die Sie bereits besitzen. Schließlich müssen Sie die DNS-Einstellungen für die Domäne ändern, um Easy DKIM für eine E-Mail-Adresse einzurichten.

Important

Für E-Mail-Adressen auf Domänen, die Sie nicht besitzen, können Sie Easy DKIM nicht einrichten. Für eine E-Mail-Adresse bei gmail.com oder hotmail.com können Sie Easy DKIM beispielsweise nicht einrichten.

Wenn Sie Easy DKIM für die Domäne, zu der die E-Mail-Adresse gehört, bereits eingerichtet haben, müssen Sie Easy DKIM für die E-Mail-Adresse nicht mehr einrichten. Wenn Sie Easy DKIM für eine Domäne einrichten, authentifiziert Amazon SES automatisch alle E-Mails von allen Adressen auf dieser

Domäne. Easy DKIM-Einstellungen für eine bestimmte E-Mail-Adresse überschreiben automatisch die Einstellungen für die Domäne, zu der die Adresse gehört.

So richten Sie Easy DKIM für eine E-Mail-Adresse ein

1. Öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management die Option Email Addresses aus.
3. Wählen Sie aus der Liste der E-Mail-Adressen die Adresse aus, für die Sie Easy DKIM einrichten möchten.
4. Wählen Sie unter DKIM die Option Generate DKIM Settings (DKIM-Einstellungen generieren) aus.
5. Kopieren Sie die drei CNAME-Datensätze, 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.
6. Fügen Sie die CNAME-Datensätze zur DNS-Konfiguration für Ihre Domäne hinzu. So aktualisieren Sie die DNS-Datensätze für Ihre Domäne:
 - Wenn Sie Route 53 als DNS-Anbieter verwenden— Führen Sie die in [Bearbeiten von Datensätzen](#) im Amazon Route 53 Entwicklerhandbuch.
 - Wenn Sie einen anderen DNS-Anbieter verwenden Verschiedene Anbieter nutzen unterschiedliche Verfahren zum Aktualisieren von DNS-Datensätzen. Weitere Informationen finden Sie in der Dokumentation Ihres DNS-Anbieters.

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.

- Wenn Sie sich nicht sicher sind, wer Ihr DNS-Anbieter ist Weitere Informationen erhalten Sie bei Ihrem Systemadministrator.

Amazon SES erkennt Änderungen an der DNS-Konfiguration in der Regel innerhalb von 72 Stunden.

Verwalten von Easy DKIM

Es gibt zwei Möglichkeiten, die Easy DKIM-Einstellungen für Ihre Identitäten zu verwalten: mithilfe der webbasierten Amazon SES S-Konsole oder mithilfe der Amazon SES-API. Sie können beide Methoden verwenden, um die DKIM-Datensätze für eine Identität abzurufen oder Easy DKIM für eine Identität zu aktivieren oder zu deaktivieren.

Abrufen von Easy DKIM-Datensätzen für eine Identität

Sie können die Easy DKIM-Datensätze für Ihre Domäne oder E-Mail-Adresse jederzeit mit der Amazon SES Konsole abrufen.

So rufen Sie die Easy DKIM-Datensätze für eine Identität mit der Konsole ab

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management (Identitätsverwaltung) den Identitätstyp aus, für den Sie die Easy DKIM-Datensätze abrufen möchten.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie Easy DKIM-Datensätze abrufen möchten.
4. Kopieren Sie im Bereich DKIM die drei CNAME-Datensätze. Die folgende Abbildung zeigt ein Beispiel für den Bereich DKIM.

▼ DKIM

DKIM settings for your domain have been generated. The information below depends on who provides your DNS service; if your DNS service is provided by a third party, you may need to create additional DNS records. [Learn more](#)

DKIM: waiting on sender verification...

DKIM Verification Status: **pending verification**

To enable DKIM signing for your domain, the records below must be entered into your DNS and allow DKIM signing at that time. Note that verification of these settings may take some time.

Name

hirjd4exampled5477y22yd23ettobiho._domainkey.example.com

v3rnz522czcl46quexamplek3efo5o6x._domainkey.example.com

y4examplexbhyhnsjcmtvzotfvqjmdqoj._domainkey.example.com

[Download Record Set as CSV »](#)

Sie können die CNAME-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.

So rufen Sie die Easy DKIM-Datensätze für eine Identität mit der AWS CLI ab

1. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses get-identity-dkim-attributes --identities "example.com"
```

Ersetzen Sie im voranstehenden Beispiel **example.com** durch die Identität, für die Sie Easy DKIM-Datensätze 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 Instance von **token1** mit dem ersten Token in der Liste, die Sie beim Ausführen des AWS-SES-Befehls `get-identity-dkim-attributes` erhalten haben. Ersetzen Sie alle Instances von **token2** durch das zweite Token in der Liste, und ersetzen Sie alle Instances 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
```

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 Easy DKIM für eine Identität

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management (Identitätsverwaltung) den Identitätstyp aus, für den Sie Easy DKIM deaktivieren möchten.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie Easy DKIM deaktivieren möchten.
4. Wählen Sie im Bereich DKIM neben DKIM: enabled (DKIM: aktiviert) die Option disable (deaktivieren) aus, wie in der folgenden Abbildung gezeigt.

▼ DKIM

DKIM settings for your domain have been generated. The information b
DNS settings depends on who provides your DNS service; if your DNS serv
update your DNS records. [Learn more](#)

DKIM: **enabled** (disable)

Sie können Easy 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.

So deaktivieren Sie Easy DKIM für eine Identität mit der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses set-identity-dkim-enabled --identity example.com --no-dkim-enabled
```

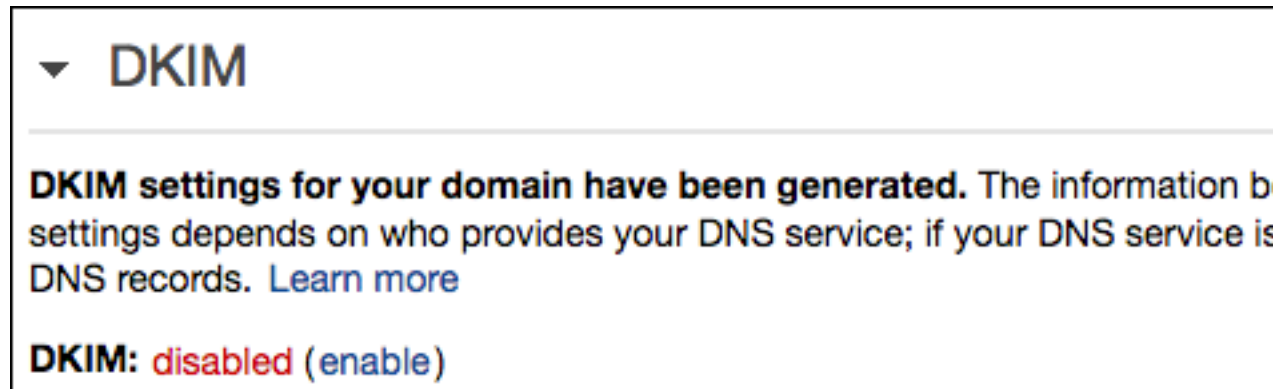
Ersetzen Sie im voranstehenden Beispiel **example.com** durch die Identität, für die Sie Easy DKIM-Datensätze deaktivieren möchten. Sie können entweder eine E-Mail-Adresse oder eine Domäne angeben.

Aktivieren von Easy DKIM für eine Identität

Wenn Sie Easy DKIM für eine Identität zuvor deaktiviert haben, können Sie es über die Amazon SES -Konsole erneut aktivieren.

So aktivieren Sie Easy DKIM für eine Identität

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management (Identitätsverwaltung) den Identitätstyp aus, für den Sie Easy DKIM aktivieren möchten.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie Easy DKIM aktivieren möchten.
4. Wählen Sie im Bereich DKIM neben DKIM: disabled (DKIM: deaktiviert) die Option enable (aktivieren) aus, wie in der folgenden Abbildung gezeigt.



Sie können Easy 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.

So aktivieren Sie Easy DKIM für eine Identität mit der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses set-identity-dkim-enabled --identity example.com --dkim-enabled
```

Ersetzen Sie im voranstehenden Beispiel **example.com** durch die Identität, für die Sie Easy DKIM-Datensätze aktivieren möchten. Sie können entweder eine E-Mail-Adresse oder eine Domäne angeben.

Bereitstellen Ihres eigenen DKIM-Authentifizierungs-Tokens in Amazon SES

Anstatt [Easy DKIM \(p. 143\)](#) 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 \(p. 150\)](#)
- [Schritt 2: Hinzufügen des öffentlichen Schlüssels zur DNS-Konfiguration für Ihre Domäne \(p. 150\)](#)
- [Schritt 3: Konfigurieren einer Domäne zur Verwendung von BYODKIM \(p. 151\)](#)

Schritt 1: Erstellen des Schlüsselpaars

Um die Funktion Bring Your Own DKIM verwenden zu können, müssen Sie zunächst ein Schlüsselpaar erstellen.

Der private Schlüssel, den Sie generieren, muss 1024-Bit-RSA-Codierung verwenden. Der private Schlüssel muss das Format PKCS #1 aufweisen.

In diesem Abschnitt erfahren Sie mehr darüber, wie Sie mit dem `openssl`-Befehl, der in den meisten Linux-, macOS - oder Unix-Betriebssystemen integriert ist, um das key pair zu erstellen.

Note

Wenn Sie einen Windows-Computer verwenden, können Sie Anwendungen von Drittanbietern verwenden, um RSA-Schlüsselpaare zu generieren. Wenn Sie eine Drittanbieter-Anwendung verwenden, muss diese in der Lage sein, ein 1024-Bit-RSA-Schlüsselpaar im PKCS #1 Format zu generieren.

So erstellen Sie das key pair über die Linux-, macOS - oder Unix-Befehlszeile

1. Geben Sie in der Befehlszeile den folgenden Befehl ein, um den privaten Schlüssel zu generieren:

```
openssl genrsa -f4 -out private.key 1024
```

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 öffentlichen Schlüssels zur DNS-Konfiguration für Ihre Domäne

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	Value
<code>selector._domainkey.example.com</code>	<code>TXT</code>	<code>p=yourPublicKey</code>

Nehmen Sie im vorherigen Beispiel Sie die folgenden Änderungen vor:

- Ersetzen Sie `selector` durch einen eindeutigen Namen, der den Schlüssel identifiziert.
- Ersetzen Sie `example.com` durch Ihre Domäne.
- Ersetzen Sie `yourPublicKey` durch den öffentlichen Schlüssel, den Sie zuvor erstellt haben.

Note

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.

Verschiedene Anbieter nutzen unterschiedliche Verfahren zum Aktualisieren von DNS-Datensätzen. Links zu der Dokumentation für mehrere gängige Anbieter werden in der nachfolgenden Tabelle aufgelistet. Diese Liste ist nicht vollständig und die Aufnahme in diese Liste ist keine Befürwortung oder Empfehlung für die Produkte oder Dienstleistungen eines Unternehmens.

DNS/Hosting-Anbieter	Link zur Dokumentation
Amazon Route 53	Bearbeiten von Datensätzen im Amazon Route 53 Entwicklerhandbuch
GoDaddy	Hinzufügen eines TXT-Datensatzes
Dreamhost	Wie füge ich benutzerdefinierte DNS-Datensätze hinzu?
Cloudflare	Verwalten von DNS-Datensätzen in CloudFlare
HostGator	Verwalten von DNS-Datensätzen mit HostGator/eNOM
Namecheap	Wie füge ich TXT/SPF/DKIM/DMARC-Datensätze für meine Domain hinzu?
Names.co.uk	Ändern der DNS-Einstellungen Ihrer Domäne
Wix	Hinzufügen oder Aktualisieren von TXT-Datensätzen in Ihrem Wix-Konto

Schritt 3: Konfigurieren 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. Domänen, die Sie bereits für die Verwendung mit Amazon SES eingerichtet haben) einrichten. Verwenden Sie zum Einrichten einer neuen Domäne die `CreateEmailIdentity`-Vorgang in der Amazon SES API. Verwenden Sie

die Operation `PutEmailIdentityDkimSigningAttributes`, um eine vorhandene Domäne zu konfigurieren.

Dieser Abschnitt enthält Verfahren zum Einrichten neuer und vorhandener Domänen mithilfe der AWS CLI. 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](#).

Option 1: Erstellen einer neuen Domänenidentität, die BYODKIM verwendet

Dieser Abschnitt enthält ein 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.

Wenn Sie eine vorhandene Domäne für die Verwendung von BYODKIM konfigurieren möchten, führen Sie stattdessen das unter [Option 2: Konfigurieren einer vorhandenen Domänen-Identität \(p. 152\)](#) beschriebene Verfahren aus.

So erstellen Sie die Identität

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 Domäne, die Sie erstellen möchten.
- Ersetzen Sie `privateKey` durch Ihren privaten Schlüssel.
- Ersetzen Sie `selector` durch den eindeutigen Selektor, den Sie beim Erstellen des TXT-Datensatzes in der DNS-Konfiguration für Ihre Domäne 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 voranstehenden Befehl `path/to/create-identity.json` durch den vollständigen Pfad zur Datei, die Sie im vorherigen Schritt erstellt haben.

Option 2: Konfigurieren einer vorhandenen Domänen-Identität

Dieser Abschnitt enthält ein 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 die Domänenidentität

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 *privateKey* durch Ihren privaten Schlüssel.
- Ersetzen Sie *selector* durch den eindeutigen Selektor, den Sie beim Erstellen des TXT-Datensatzes in der DNS-Konfiguration für Ihre Domäne 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:

- Ersetzen Sie *path/to/update-identity.json* durch den vollständigen Pfad zu der Datei, die Sie im vorherigen Schritt erstellt haben.
- Ersetzen Sie *example.com* durch die Domäne, die aktualisiert werden soll.

Überprüfen des DKIM-Status für eine Domäne, die BYODKIM verwendet

Nachdem Sie eine Domäne für die Verwendung von BYODKIM konfiguriert haben, können Sie mithilfe der Operation `GetEmailIdentity` überprüfen, ob DKIM ordnungsgemäß konfiguriert wurde.

So überprüfen Sie den DKIM-Status einer Domäne

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 get-email-identity --email-identity example.com
```

Ersetzen Sie im voranstehenden Befehl *example.com* durch Ihre Domäne.

Dieser Befehl gibt ein JSON-Objekt zurück, das einen Abschnitt enthält, der dem folgenden Beispiel ähnelt.

```
{
  ...
  "DkimAttributes": {
    "SigningAttributesOrigin": "EXTERNAL",
    "SigningEnabled": true,
    "Status": "SUCCESS",
    "Tokens": [ ]
  },
  ...
}
```

BYODKIM ist ordnungsgemäß für die Domäne konfiguriert, wenn alle folgenden Voraussetzungen erfüllt sind:

- Der Wert der Eigenschaft `SigningAttributesOrigin` lautet `EXTERNAL`.

- Der Wert von `SigningEnabled` ist `true`.
- Der Wert von `Status` ist `SUCCESS`.

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. Nach dem Erstellen der Nachricht und der DKIM-Signatur können Sie mit der [SendRawEmail-API](#) Ihre Nachricht versenden.

Wenn Sie Ihre E-Mails manuell signieren möchten, beachten Sie die folgenden Aspekte:

- Jede Nachricht, die Sie mit Amazon SES senden, enthält einen DKIM-Header, der auf eine Signaturdomäne von `amazonses.com` Das heißt, es enthält die folgende Zeichenfolge: `d=amazonses.com`) enthalten. Wenn Sie Ihre Nachrichten manuell signieren, sollten Ihre Nachrichten zwei DKIM-Header: einer für Ihre Domäne und einer für `amazonses.com`.
- DKIM-Signaturen, die Sie manuell zu Ihren Nachrichten hinzufügen, werden von 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.
- Unterzeichnen Sie die folgenden Felder nicht: `Rückgabepath`, `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. Der Dokumentation zu Ihrem E-Mail-Client können Sie entnehmen, welche Felder standardmäßig signiert werden.

Einhaltung von DMARC mit Amazon SES

Domain-based Message Authentication, Reporting and Conformance (DMARC) ist ein E-Mail-Authentifizierungs-Protokoll, das Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) verwendet, um E-Mail-Spoofing zu erkennen. Zur Einhaltung von DMARC müssen Nachrichten über SPF, DKIM oder beides authentifiziert werden.

Dieses Thema enthält Informationen zur Konfiguration von Amazon SES, sodass Ihre gesendeten E-Mails sowohl SPF als auch DKIM erfüllen. Wenn Ihre E-Mails eines dieser Authentifizierungssysteme erfüllen, erfüllen sie auch DMARC. Informationen zur DMARC-Spezifizierung finden Sie unter <http://www.dmarc.org>.

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 [Arbeiten mit 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	Value
<code>_dmarc.example.com</code>	TXT	<code>"v=DMARC1;p=quarantine;pct=25;rua=ma</code>

In Klartext: E-Mail-Anbieter werden durch diese Richtlinie angewiesen, die folgenden Schritte auszuführen:

- Suchen Sie alle E-Mails mit der "From" (Von)-Domäne `example.com`, die keine SPF- oder DKIM-Authentifizierung bestanden haben.
- Stellen Sie 25 % der E-Mails, die die Authentifizierung nicht bestanden haben, unter Quarantäne. Senden Sie sie dazu in den Spam-Ordner (Sie können auch mit `p=none` nichts unternehmen oder die Nachrichten mit `p=reject` direkt ablehnen).
- Senden Sie Berichte über alle E-Mails mit fehlgeschlagener Authentifizierung in eine Digest-Datei (d. h. einem Bericht, der Daten für einen bestimmten Zeitraum sammelt, anstatt für jedes Ereignis einzelne Berichte zu senden). 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.

Umfassende Spezifikationen des DMARC-Systems finden Sie unter [RFC 7489](#) auf der IETF-Website. Abschnitt 6.3 dieses Dokuments enthält eine vollständige Liste der Tags, die Sie zum Konfigurieren der DMARC-Richtlinie für Ihre Domäne verwenden können.

Einhaltung von DMARC über SPF

Damit eine E-Mail basierend auf SPF DMARC erfüllt, müssen beide der folgenden Bedingungen erfüllt sein:

- Die E-Mail muss ein SPF-Prüfung bestehen.
- Die Domäne in der "From"-Adresse des E-Mail-Headers muss mit der MAIL FROM-Domäne übereinstimmen, die der sendende Mail-Server für den empfangenden Mail-Server angibt. Wenn die DMARC-Richtlinie der Domäne für SPF eine enge Übereinstimmung vorsieht, müssen sich die "From"- und MAIL FROM-Domänen genau entsprechen. Wenn die DMARC-Richtlinie der Domäne für SPF eine lockere Übereinstimmung vorsieht, kann es sich bei der MAIL FROM-Domäne um eine Unterdomäne der Domäne im From-Header handeln.

Gehen Sie wie folgt vor, um diese Anforderungen zu erfüllen:

- Befolgen Sie die Anleitung unter [the section called "Einrichten einer benutzerdefinierten MAIL FROM-Domäne" \(p. 72\)](#), um eine benutzerdefinierte MAIL FROM-Domäne einzurichten.
- Stellen Sie sicher, dass Ihre sendende Domäne eine lockere Richtlinie für SPF verwendet. Wenn Sie die Richtlinienausrichtung Ihrer Domäne nicht geändert haben, wird standardmäßig eine lockere Richtlinie verwendet.

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:

```
nslookup -type=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-Suchtool wie den [DMARC Inspector](#) von der dmarcian-Website oder das [DMARC Check](#)-Tool von der Proofpoint-Website verwenden, um die Richtlinienausrichtung Ihrer Domäne für SPF zu bestimmen.

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.
- Die "From"-Adresse im E-Mail-Header muss mit der d=Domäne in der DKIM-Signatur übereinstimmen. Wenn die DMARC-Richtlinie der Domäne eine enge Übereinstimmung für DKIM vorsieht, müssen sich diese Domänen genau entsprechen. Wenn die DMARC-Richtlinie der Domäne eine lockere Übereinstimmung für DKIM vorsieht, kann es sich bei der d=Domäne um eine Unterdomäne der "From"-Domäne handeln.

Gehen Sie wie folgt vor, um diese Anforderungen zu erfüllen:

- Richten Sie Easy DKIM anhand der Anleitung unter [the section called "Easy DKIM" \(p. 143\)](#) 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 \(p. 154\)](#). 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 Ihre sendende Domäne eine lockere Richtlinie für DKIM verwendet. Wenn Sie die Richtlinienausrichtung Ihrer Domäne nicht geändert haben, wird standardmäßig eine lockere Richtlinie verwendet.

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:

```
nslookup -type=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-Suchtool wie den [DMARC Inspector](#) von der dmarcian-Website oder das [DMARC Check](#)-Tool von der Proofpoint-Website verwenden, um die Richtlinienausrichtung Ihrer Domäne für DKIM zu bestimmen.

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. Sendekontingente kommen allen Amazon SES Kunden zugute, da sie dazu beitragen, die vertrauensvolle

Beziehung 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:

- **Maximale tägliche Sendungen**— Die maximale Anzahl von E-Mails, die Sie in einem Zeitraum von 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 Sendeaufforderung akzeptiert und Ihre E-Mail gesendet.

Wenn das Senden einer Nachricht das tägliche Maximum für Ihr Konto überschreiten würde, wird Ihr Aufruf an Amazon SES abgelehnt.

- **Maximale Senderate**— Die maximale Anzahl von 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.

Ihre Amazon SES S-Versandkontingente gelten für jede AWS Region getrennt. Weitere Informationen zur Verwendung von Amazon SES in mehreren AWS Regionen finden Sie unter [Regionen und Amazon SES](#) (p. 494).

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 [Verlassen der Amazon SES -Sandbox](#) (p. 79).

Wenn Ihr Konto aus der -Sandbox entfernt wurde, können Sie jederzeit zusätzliche Kontingenterhöhungen anfordern, indem Sie im AWS Support Center einen neuen Fall erstellen. Weitere Informationen finden Sie unter [Erhöhen Ihrer Amazon SES Versandkontingente](#) (p. 159).

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 Versandkontingente](#) (p. 159).
- Informationen zu den Fehlern, die Ihre Anwendung bei Erreichen der Sendekontingente erhält, finden Sie unter [Fehler im Zusammenhang mit den Sendekontingenten für Ihr Amazon SES Konto](#) (p. 161).
- Weitere Informationen darüber, wie Sie Ihre Sendekontingente mithilfe der Amazon SES Konsole oder der Amazon SES-API überwachen können, finden Sie unter [Überwachen Ihrer Amazon SES Versandkontingente](#) (p. 158).

Überwachen Ihrer Amazon SES Versandkontingente

Sie können Ihre Sendekontingente mit Hilfe der Amazon SES S-Konsole oder über die Amazon SES-API überwachen — durch den direkten oder indirekten Aufruf der Query (HTTPS) -Schnittstelle über eine [AWS SDK](#), die [AWS Command Line Interface](#), oder die [AWS Tools for Windows PowerShell](#).

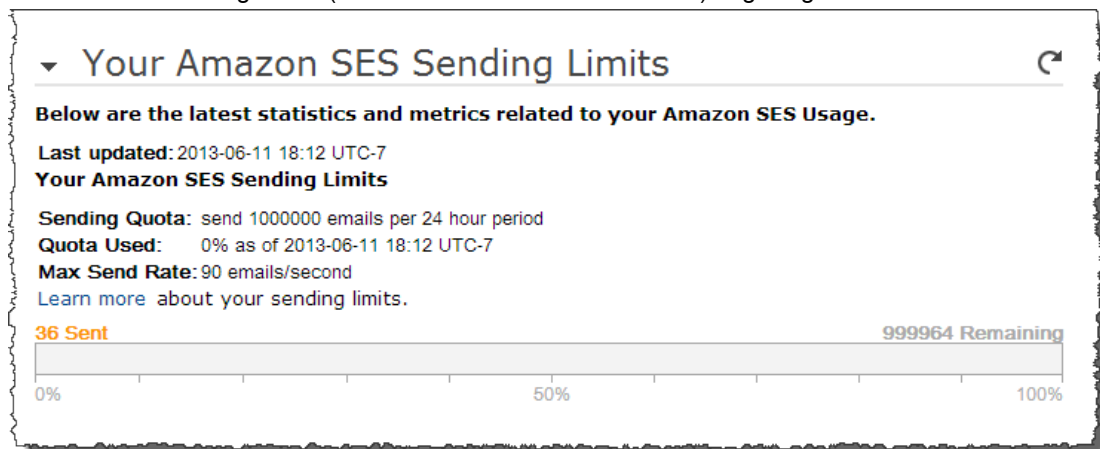
Important

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 Versandkontingente \(p. 159\)](#) 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.

Überwachen Ihrer Versandkontingente mit der Amazon SES Konsole

Im folgenden Verfahren erfahren Sie, wie Sie Ihre Sendekontingente mithilfe der Amazon SES -Konsole anzeigen können.

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich Sending Statistics aus. Ihre Sendekontingente werden unter Your Amazon SES Sending Limits (Ihre Sendelimits für Amazon SES) angezeigt.



3. Um die Anzeige zu aktualisieren, wählen Sie Refresh aus.

Überwachung Ihrer Sendekontingente mit der Amazon SES API

Die Amazon SES API stellt die `getSendQuota`-Aktion, 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](#).

Erhöhen Ihrer Amazon SES Versandkontingente

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— Senden Sie Inhalte, die der Empfänger wünscht und erwartet. Sie senden Kunden, die Ihre E-Mails nicht öffnen, keine weiteren E-Mails mehr.
- Sie senden den tatsächlichen Produktionsinhalt— 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 senden in der Nähe Ihres aktuellen Kontingents— Wenn Sie sich für eine automatische Kontingenterhöhung qualifizieren möchten, sollte Ihre tägliche E-Mail-Menge regelmäßig das tägliche Maximum für Ihr Konto erreichen, ohne es zu überschreiten.
- Sie haben niedrige Absprung- und Reklamationsraten— Minimieren 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.

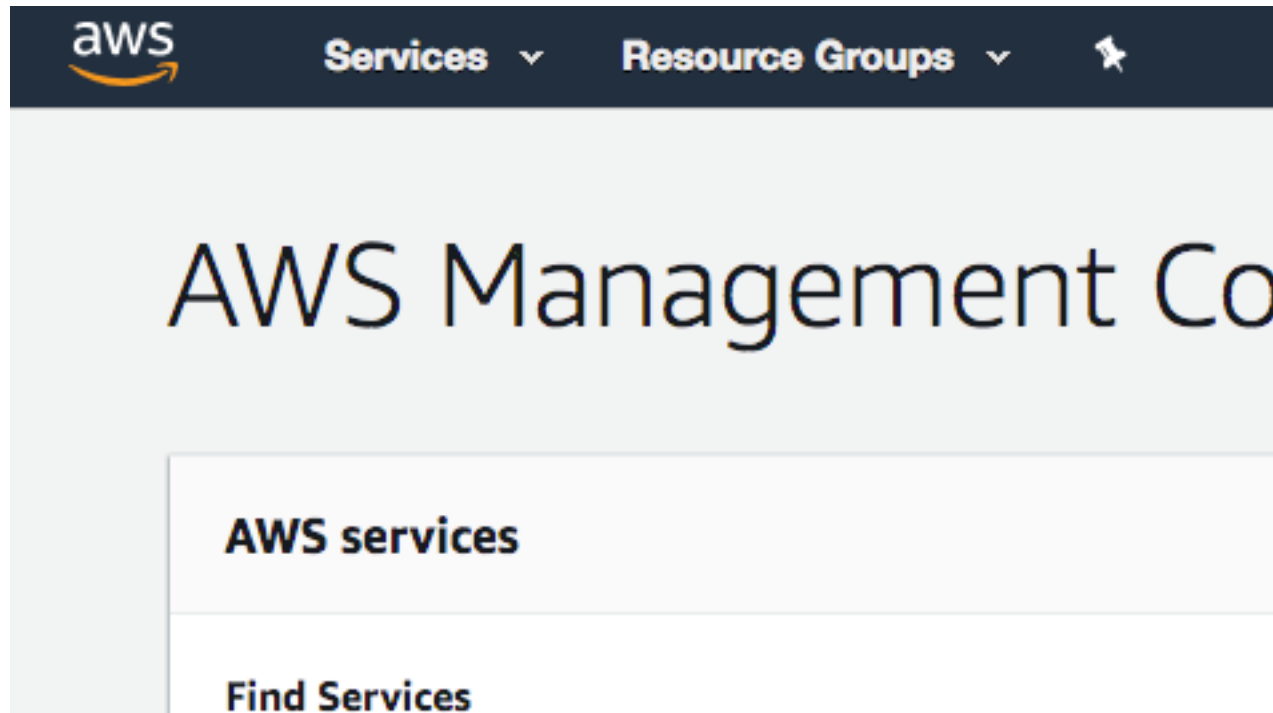
Wenn Ihre aktuellen Sendekontingente Ihren Bedürfnissen nicht entsprechen und wir die Kontingente nicht automatisch erhöhen, können Sie eine Erhöhung anfordern. Weitere Informationen zum Anfordern einer Erhöhung der Sendekontingente finden Sie unter [Öffnen eines Falls zur Erhöhung der Amazon SES Kontingente](#) (p. 159).

Öffnen eines Falls zur Erhöhung der Amazon SES Kontingente

Um höhere Sendekontingente für Amazon SES zu beantragen, öffnen Sie einen Fall im Support Center, indem Sie die folgenden Schritte abschließen.

So fordern Sie höhere Sendekontingente an

1. Melden Sie sich beim an.AWS Management Consoleum <https://console.aws.amazon.com/>.
2. Wählen Sie im Menü Support (Support) die Option Support Center (Support-Center) aus, wie in der folgenden Abbildung dargestellt.



3. Wählen Sie auf der Registerkarte My support cases (Meine Support-Fälle) die Option Create case (Fall erstellen) aus.
4. Wählen Sie unter Create case (Fall erstellen) die Option Service limit increase (Erhöhung des Service Limits) aus.
5. Führen Sie unter Case classification (Fallklassifizierung) die folgenden Abschnitte aus:
 - Wählen Sie als Limit Type (Limit-Typ) die Option SES Service Limits (SES-Service Limits) aus.
 - Wählen Sie als Mail Type (E-Mail-Typ) den E-Mail-Typ aus, den Sie senden möchten. Wenn mehr als ein Wert zutrifft, wählen Sie die Option aus, die für die meisten der E-Mails gilt, die Sie senden möchten.
 - Geben Sie als Website URL (Website-URL) die URL der Website ein. Durch die Bereitstellung dieser Informationen können wir besser einschätzen, welche Art von Inhalt Sie senden möchten.
 - Für Meine E-Mail-Sendefunktionen entsprechen den AWS -Servicebedingungen und AUP Wählen Sie die Option aus, die Ihrem Anwendungsfall entspricht.
 - Wählen Sie unter I only send to recipients who have specifically requested my mail (Ich sende nur an Empfänger, die meine Mail explizit angefordert haben) die Option aus, die Ihrem Anwendungsfall entspricht.
 - Wählen Sie unter I have a process to handle bounces and complaints (Ich habe einen Prozess für die Verarbeitung von unzustellbaren E-Mails und Beschwerden) die Option aus, die Ihrem Anwendungsfall entspricht.
6. Führen Sie unter Requests (Anforderungen) die folgenden Abschnitte aus:
 - Für Region Wählen Sie die AWS Region aus, für die Ihre Anfrage gilt.
 - Wählen Sie als Limit die Art der Kontingenterhöhung aus, die Sie anfordern möchten. Sie können aus den folgenden Optionen auswählen:
 - Gewünschte maximale Senderate— Wählen Sie diese Option aus, wenn Sie eine Erhöhung der Anzahl der E-Mails anfordern möchten, die Ihr Konto pro 24-Stunden-Zeitraum in der ausgewählten Region senden kann.

Gewünschte maximale Senderate— Wählen Sie diese Option aus, wenn Sie eine Erhöhung der Anzahl der E-Mails anfordern möchten, die Ihr Konto pro Sekunde in der ausgewählten Region senden kann.

- Geben Sie unter New limit value (Neuer Grenzwert) das Kontingent ein, das Sie erhöhen möchten. Fordern Sie nur so viel an, wie Sie benötigen. Denken Sie daran, dass Sie nicht garantiert die angeforderte Menge erhalten.

Note

Wenn Sie sowohl eine Quota-Erhöhung und ein Senden-RATE, wenn Sie eine Erhöhung des Sendekontingents in einer anderen AWS Region anfordern möchten, wählen Sie Weitere Anfrage hinzufügen. Wiederholen Sie dann diesen Schritt.

7. **UNDER** Beschreibung des Falles, für Anwendungsfall Beschreiben Sie dann, wie Sie Amazon SES zum Senden von E-Mails verwenden möchten. Beantworten Sie die folgenden Fragen, damit wir Ihre Anfrage bearbeiten können:
 - Wie werden Sie Ihre Mailingliste zusammenstellen bzw. von wo erhalten Sie diese?
 - Wie werden Sie mit Beschwerden und unzustellbaren Nachrichten umgehen?
 - Wie können Empfänger sich gegen den Erhalt Ihrer E-Mail entscheiden?
 - Wie haben Sie die neue Senderate oder Sendequote ermittelt, die Sie in dieser Anfrage angegeben haben?

Falls wir bei der Bewertung Ihres Falls zusätzliche Informationen beachten sollen, geben Sie diese ebenfalls in diesem Abschnitt an.

8. Wählen Sie unter Contact options (Kontaktoptionen) als Preferred contact language (Bevorzugte Kontaktsprache) aus, ob Sie in diesem Fall auf English (Englisch) oder Japanese (Japanisch) kommunizieren möchten.
9. Wenn Sie fertig sind, klicken Sie auf Submit.

Sie erhalten auf Ihre Anfrage innerhalb von 24 Stunden eine erste Reaktion vom AWS Support-Team.

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.

Wenn Ihr Anwendungsfall gegen unsere Richtlinien verstößt, können wir Ihrer Anfrage möglicherweise nicht nachkommen.

Fehler im Zusammenhang mit den 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. Außerdem stellt Amazon SES 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 [Behandeln eines Fehlers „Throttling — Maximum sending rate exceeded“](#) im AWS Messaging and Targeting Blog.

Sendegrenzen mit der Amazon SES API erreichen

Wenn Sie versuchen, eine E-Mail mit der Amazon SES -API (oder einem AWS S-SDK) zu senden, Sie aber bereits die Sendelimits Ihres Kontos überschritten haben, erzeugt API eine `ThrottlingException`-Fehler. 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 Sendeauforderung zu senden.

Sendungslimits mit SMTP erreichen

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.

Verwenden der Sendeautorisierung mit Amazon SES

Sie können Amazon SES so konfigurieren, dass andere Benutzer E-Mails von Adressen oder Domänen, deren Eigentümer Sie sind (Ihre-Identitäten) mit ihren eigenen Amazon SES Konten. Anhand dieser Funktion, die als Sendeautorisierung bezeichnet wird, behalten Sie die Kontrolle über Ihre Identitäten, sodass Sie Berechtigungen jederzeit ändern oder widerrufen können. Als Inhaber eines Unternehmens können Sie beispielsweise mithilfe der Sendeautorisierung einen Dritten (z. B. ein E-Mail-Marketing-Unternehmen) berechtigen, E-Mails von einer Domäne zu senden, die Sie besitzen.

Wenn Sie eine Person autorisieren möchten, in Ihrem Auftrag E-Mails senden zu können, sind Sie ein Identitätseigentümer. Wenn Sie ein Identitätseigentümer sind, empfehlen wir Ihnen, die folgenden Abschnitte zu lesen:

- [Übersicht über die -Sendeautorisierung \(p. 163\)](#)
- [Sendeautorisierungsrichtlinien \(p. 165\)](#)
- [Beispiele von Sendeautorisierungsrichtlinien \(p. 170\)](#)
- [Aufgaben des Identitätseigentümers \(p. 175\)](#)

Wenn Sie berechtigt sind, E-Mails im Auftrag einer anderen Person zu senden, sind Sie ein stellvertretender Sender. Wenn Sie ein stellvertretender Sender sind, empfehlen wir Ihnen, die folgenden Abschnitte zu lesen:

- [Übersicht über die -Sendeautorisierung \(p. 163\)](#)
- [Delegieren der Senderaufgaben \(p. 182\)](#)

Note

Sie können auch mithilfe von IAM-Richtlinien den Zugriff auf Amazon SES steuern. Die IAM-Richtlinien regeln, welche Aufgaben einzelne IAM-Benutzer ausführen können, während die Richtlinien zur Sendeautorisierung regeln, wie individuelle verifizierte Identitäten verwendet werden können. Darüber hinaus können nur Sendeautorisierungsrichtlinien kontenübergreifenden Zugriff gewähren. Weitere Informationen zur Verwendung von IAM-Richtlinien mit Amazon SES finden Sie unter [Steuern des Zugriffs auf Amazon SES \(p. 431\)](#).

Übersicht über Amazon SES Sendeautorisierung

Dieses Thema bietet eine Übersicht über den Vorgang der Sendeautorisierung und erklärt, wie die -Funktionen zum Senden von E-Mails in Amazon SES, z. B. Sendekontingente und Benachrichtigungen, in Bezug auf die Sendeautorisierung funktionieren.

In diesem Abschnitt werden die folgenden Begriffe verwendet:

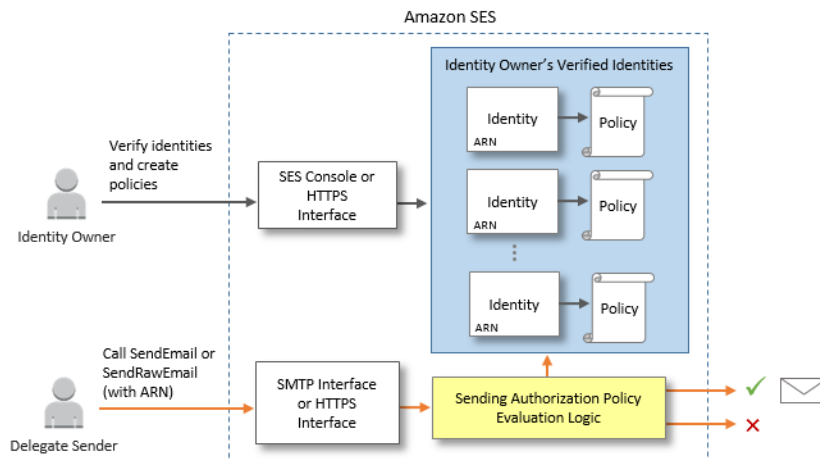
- **Identität** — Eine E-Mail-Adresse oder Domäne, die -Benutzer zur Versendung von E-Mails verwenden
- **Identität des Eigentümers** — Ein Amazon SES Benutzer, der aufgrund der unter beschriebenen Verfahren die verifizierte Eigentümerschaft über eine E-Mail-Adresse oder Domäne besitzt [Verifizieren von Identitäten \(p. 52\)](#).
- **Delegieren von Sendern** — Eine Entität, die berechtigt ist, von einer Identität, deren Eigentümer sie nicht ist, E-Mails zu senden. Ein AWS Konto, ein AWS Identity and Access Management Ein AWS -Service kann über Kontoübergreifender-Autorität.
- **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, Amazon-Ressourcenname)** — Eine standardisierte Kennzeichnung, die eine AWS-Ressource über alle AWS-Services hinweg identifiziert. Im Fall einer Sendeautorisierung, ist die Ressource die Identität, deren Verwendung der Identitätseigentümer für den stellvertretenden Sender beabsichtigt. Hier sehen Sie ein Beispiel für einen ARN `arn: aws: ses: us-west-2:123456789012: Identität/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 Identitätseigentümer überprüft eine Identität mit Amazon SES anhand der Amazon SES -Konsole oder der Amazon SES -API. Weitere Informationen über das Verifizierungsverfahren finden Sie unter [Verifizieren von Identitäten \(p. 52\)](#).
2. Der stellvertretende Sender gibt dem Identitätseigentümer die AWS Konto-ID, den IAM-Benutzer-ARN oder den AWS-Servicenamen der Entität an, die das Versenden ausführt.
3. Der Identitätseigentümer erstellt eine Richtlinie für die Sendeautorisierung und fügt sie anhand der Amazon SES-Konsole oder der Amazon SES -API der Identität an.
4. Der Identitätseigentümer gibt dem stellvertretenden Sender den ARN der Identität, damit der stellvertretende Sender den ARN beim Senden der E-Mail dem Amazon SES bereitstellen kann.
5. Der stellvertretende Sender richtet Unzustellbarkeits- und Beschwerdebenachrichtigungen ein. Der Identitätseigentümer kann ebenfalls E-Mail-Feedback-Benachrichtigungen für Unzustellbarkeits- und Beschwerdeereignisse einrichten. Sowohl der Identitätseigentümer als auch der stellvertretende Sender kann auch [Ereignisveröffentlichung \(p. 313\)](#) verwenden, um Sendeereignisdaten zu erfassen.

Note

Wenn der Identitätseigentümer Sendeereignisbenachrichtigungen deaktiviert, muss der stellvertretende Sender Ereignisveröffentlichung einrichten, um Unzustellbarkeits- und Beschwerdeereignisse in einem Amazon SNS -Thema oder einem Kinesis Data 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 Identitätseigentümer noch der stellvertretende Sender eine Methode zum Senden von Benachrichtigungen für Unzustellbarkeits- und Beschwerdeereignisse einrichten, sendet Amazon SES Ereignisbenachrichtigungen automatisch per E-Mail an die Adresse im Feld Rücksendepfad der E-Mail (oder die Adresse im Feld Quelle, wenn Sie keine Rücksendung angegeben haben. -Pfadadresse), auch wenn der Identitätsbesitzer die E-Mail-Feedback-Weiterleitung deaktiviert hat.

6. Der stellvertretende Sender versucht, im Namen des Identitätseigentümers eine E-Mail über Amazon SES zu senden, indem er den ARN der Identität des Identitätseigentümers 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 „From“ - und „Return Path“ -Adresse autorisiert ist. Andernfalls gibt Amazon SES einen Fehler zurück und die Nachricht wird nicht akzeptiert.

7. Wenn der Identitätseigentümer die Autorisierung des stellvertretenden Senders aufheben muss, muss der Identitätseigentümer die Richtlinie für die Sendeautorisierung bearbeiten oder die Richtlinie vollständig löschen. Der Identitätseigentümer kann jede dieser Aktionen über die Amazon SES -Konsole oder die Amazon SES -API ausführen.

Weitere Informationen darüber, wie der Identitätseigentümer oder der stellvertretende Sender diese Aufgaben ausführt, finden Sie unter [Aufgaben des Identitätseigentümers \(p. 175\)](#) bzw. [Delegieren der Senderaufgaben \(p. 182\)](#).

Zuordnung der Funktionen für den E-Mail-Versand

Es ist wichtig, die Rolle des stellvertretenden Senders und des Identitätseigentümers in Bezug auf die Funktionen des -E-Mail-Versands von Amazon SES zu verstehen. Diese Funktionen umfassen beispielsweise die tägliche Sendequote, Unzustellbarkeitsnachrichten und Beschwerden, DKIM-Signatur, Feedback-Weiterleitung usw. Die Zuordnung erfolgt folgendermaßen:

- **Sendequote**— E-Mails, die über die Identitäten des Identitätseigentümers gesendet werden, werden auf die -Sendekontingente des stell
- **Bounces und Reklamationen**— 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-Unterschrift**Wenn der Identitätseigentümer 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 Identitätseigentümer kann steuern, ob die E-Mails mit einer DKIM-Signatur versehen werden.
- **Benachrichtigungen**— Sowohl der Identitätseigentümer als auch der stellvertretende Sender kann Benachrichtigungen für Unzustellbarkeitsnachrichten und Beschwerden einrichten. Der E-Mail-Identitätseigentümer kann auch die Weiterleitung von E-Mail-Feedback aktivieren. Weitere Informationen zum Einrichten von Benachrichtigungen finden Sie unter [Überwachen Ihrer Amazon SES Versandaktivitäten \(p. 282\)](#).
- **Verifizierung**— Identitätsinhaber sind dafür verantwortlich, das Verfahren in [Verifizieren von Identitäten \(p. 52\)](#), um zu gewährleisten, dass sie die E-Mail-Adressen und Domänen auch tatsächlich besitzen, bevor sie stellvertretende Sender zu deren Verwendung autorisieren. Stellvertretende Sender müssen speziell für die Sendeautorisierung keine E-Mail-Adressen oder Domänen bestätigen.
- **AWS Regions (AWS-Regionen)**— Der stellvertretende Sender muss die E-Mails von der AWS Region senden, in der der Identitätseigentümer verifiziert ist. 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 Identitätseigentümers sendet, werden dem stellvertretenden Sender in Rechnung gestellt.

Amazon SES deauthorisierungsrichtlinien

Um ein anderes AWS Konto, einen anderen Identity and Access Management- (IAM) Benutzer oder einen anderen AWS-Service zu berechtigen, in Ihrem Namen über Amazon SES E-Mails zu senden, erstellen Sie eine Senden der Autorisierungsrichtlinie. Hierbei handelt es sich um ein JSON-Dokument, das Sie einer in Ihrem Besitz befindlichen Identität anfügen. Die Richtlinie führt explizit auf, wem Sie die Berechtigung erteilen, für diese Identität E-Mails zu senden, und unter welchen Bedingungen. Mit Ausnahme von Ihnen und den Entitäten, denen Sie in den Richtlinien ausdrücklich die Berechtigung erteilen, wird allen anderen Sendern das Senden von E-Mails verweigert. Einer Identität kann keine Richtlinie, eine Richtlinie oder mehrere Richtlinien angefügt werden. Eine Richtlinie kann auch mehrere Anweisungen enthalten und so die gleiche Wirkung wie mehrere Richtlinien erzielen.

Richtlinien können einfach gehalten oder so konfiguriert sein, dass sie eine differenzierte Kontrolle ermöglichen. Zum Beispiel, wenn Sie `example.com` können Sie eine einfache Richtlinie schreiben, mit der Sie die AWS ID 123456789012 berechtigen, von dieser Domäne E-Mails zu versenden. Eine ausführlichere Richtlinie könnte beispielsweise festlegen, dass die AWS-ID 123456789012 nur von `user@example.com` E-Mails versenden kann und dies nur innerhalb eines angegebenen Zeitraums.

-Sendeautorisierungsrichtlinien von Amazon SES gelten für E-Mail versendende APIs (`SendEmail`, `SendRawEmail`, `SendTemplatedEmail`, und `SendBulkTemplatedEmail` (nur)). Sie berechtigen Benutzer nicht, auf andere Weise auf Ihr AWS Konto zuzugreifen.

Richtlinienstruktur

Bei jeder Sendeaufisierungsrichtlinie 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

Im folgenden Beispiel wird AWS Konto-ID verliehen. 123456789012 Berechtigung zum Senden von der verifizierten Domäne `example.com`.

```
{
  "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:SendEmail",
        "ses:SendTemplatedEmail",
        "ses:SendRawEmail",
        "ses:SendBulkTemplatedEmail"
      ]
    }
  ]
}
```

Sie finden weitere Beispiele von Sendeaufisierungsrichtlinien unter [Beispiele von Sendeaufisierungsrichtlinien](#) (p. 170).

Richtlinienelemente

Dieser Abschnitt beschreibt die Elemente, aus denen sich die Sendeaufisierungsrichtlinien zusammensetzen. 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.

Weitere Informationen über die Syntax der Elemente finden Sie unter [Grammatik der IAM-Richtliniensprache](#) im IAM-Benutzerhandbuch.

Richtlinienweite Informationen

Es gibt zwei richtlinienweite Elemente: `Id` und `Version`. Die folgende Tabelle enthält Informationen über diese Elemente.

Name	Beschreibung	Erforderlich	Zulässige Werte
<code>Id</code>	Kennzeichnet die Richtlinie eindeutig.	Nein	Jede Zeichenfolge
<code>Version</code>	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

Sendeautorisierungsrichtlinien erfordern mindestens eine Anweisung. Jede Anweisung kann die in der folgenden Tabelle beschriebenen Elementen enthalten.

Name	Beschreibung	Erforderlich	Zulässige Werte
<code>Sid</code>	Kennzeichnet die Anweisung eindeutig.	Nein	Jede Zeichenfolge.
<code>Effect</code>	Gibt das Ergebnis an, das die Richtlinienanweisung zum Bewertungszeitpunkt zurückgeben soll.	Ja	"Allow" oder "Deny".
<code>Resource</code>	Gibt die Identität an, auf die die Richtlinie zutrifft. Dies ist die E-Mail-Adresse oder Domäne, für die der Identitätseigentümer dem stellvertretenden Sender die Berechtigung erteilt.	Ja	Der Amazon-Ressourcenname (ARN) der E-Mail-Identität.
<code>Principal</code>	Gibt das AWS Konto, den IAM-Benutzer oder den AWS-Service an, auf das/den sich die Berechtigung in der Anweisung bezieht.	Ja	Eine gültige AWS Konto-ID, ein gültiger IAM-Benutzer-ARN oder AWS -Service. AWS Konto-IDs und IAM-Benutzer-ARNs werden mithilfe von "AWS" (z. B. "AWS" : ["123456789012"] oder ".AWS" : ["arn:aws:iam::123456789012:r enthalten. AWS-Servicenamen werden mithilfe von "Service" (z. B. "Service" :

Name	Beschreibung	Erforderlich	Zulässige Werte
			["cognito-idp.amazonaws.com"]) angegeben. Beispiele für das Format des IAM-Benutzer-ARNs finden Sie im Allgemeine AWS-Referenz.
Action	Gibt die für das Senden der E-Mail verantwortliche Aktion an, für die die Anweisung gilt.	Ja	"ses:SendEmail", "ses:SendRawEmail", "ses:SendTemplatedEmail", "ses:SendBulkTemplatedEmail" Sie können eine oder mehrere dieser Operationen angeben. Sie können auch "ses: Send*" angeben, um alle diese Operationen zu umfassen. Wenn der stellvertretende Sender beabsichtigt, E-Mails über die SMTP-Schnittstelle zu senden, müssen Sie "ses: SendRawEmail" angeben oder "ses: Send*" verwenden.
Condition	Gibt alle Einschränkungen oder Details über die Berechtigung an.	Nein	Weitere Informationen über Bedingungen finden Sie im Anschluss an diese Tabelle.

Conditions

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 `DateLessThan`. Sie verwenden den Schlüssel `aws:CurrentTime` und legen den Wert mit `2019-07-30T00:00:00Z` fest.

Sie können alle AWS-weiten Schlüssel verwenden, die unter [Verfügbare Schlüssel](#) im IAM-Benutzerhandbuch oder Sie können einen der folgenden speziellen Schlüssel für Amazon SES verwenden:

Bedingungsschlüssel	Beschreibung
<code>ses:Recipients</code>	Beschränkt die Empfängeradressen, einschließlich der Adressen "To", "CC" und "BCC".

Bedingungsschlüssel	Beschreibung
<code>ses:FromAddress</code>	Beschränkt die "From"-Adresse.
<code>ses:FromDisplayName</code>	Beschränkt den Inhalt der Zeichenfolge, die als der "From"-Anzeigenname verwendet wird (manchmal auch "Friendly from" genannt). So lautet beispielsweise der Anzeigenname für "John Doe <johndoe@example.com>" John Doe.
<code>ses:FeedbackAddress</code>	Beschränkt die "Return Path"-Adresse. Dies ist die Adresse, an die Unzustellbarkeitsnachrichten und Beschwerden an Sie anhand von Feedback-E-Mails weitergeleitet werden können. Weitere Informationen zum Weiterleiten von Feedback per E-Mail finden Sie unter Per E-Mail gesendete Amazon SES S-Benachrichtigungen (p. 289).

Sie können die `BerechtigungStringEqualsundStringLike` Bedingungen mit Amazon SES Schlüsseln. 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.com` endet:

```
"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 Festlegen von Bedingungen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.

Richtlinienanforderungen

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.
- Identitätseigentümer 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.

Beispiele von Amazon SES Sendeautorisierungsrichtlinien

In der Sendeautorisierung können Sie die spezifischen Bedingungen angeben, unter denen stellvertretende Sender in Ihrem Namen E-Mails senden dürfen.

Die folgenden Beispiele zeigen Ihnen, wie Sie die Richtlinien erstellen müssen, um die verschiedenen Aspekte des Sendens zu kontrollieren:

- [Angaben des stellvertretenden Senders \(p. 170\)](#)
- [Beschränken der "From"-Adresse \(p. 172\)](#)
- [Beschränken der Zeit, zu der der stellvertretende Sender E-Mails senden kann \(p. 172\)](#)
- [Beschränkung des E-Mail-Versands \(p. 173\)](#)
- [Beschränken des Anzeigenamens des E-Mail-Absenders \(p. 174\)](#)
- [Verwenden mehrerer Anweisungen \(p. 174\)](#)

Angeben des stellvertretenden Senders

Die Prinzipal Wenn es sich um die Entität handelt, der Sie die Berechtigung erteilen, kann es sich um ein AWS Konto, einen AWS Identity and Access Management (IAM) -Benutzer oder einen AWS -Service.

Das folgende Beispiel zeigt eine einfache Richtlinie, die AWS ID 123456789012, um eine E-Mail von der verifizierten Identität zu senden `example.com` (das Eigentum des AWS Kontos ist 888888888888) enthalten. Die `Condition`-Anweisung in dieser Richtlinie erlaubt nur den Delegaten (d. h. die AWS ID 123456789012), um eine E-Mail von der Adresse zu senden `marketing+.*@example.com` wobei `*` eine Zeichenfolge darstellt, die der Sender nach `marketing+`.

```
{
  "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 E-Mails zu sendenexample.com. IAM-Benutzer werden durch ihren Amazon-Ressourcennamen (ARN) angegeben.

```
{
  "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 E-Mails zu sendenexample.com.

```
{
  "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"
      ]
    }
  ]
}
```

Die folgende Beispielrichtlinie erteilt allen -Konten innerhalb einer AWS Organisation die Berechtigung, von der Identität example.com E-Mails zu senden. Die AWS Organisation wird mit dem [PrincipalOrgID](#)-Bedingungsschlüssel.

```
{
  "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-xxxxxxxxxxxxx"
    }
  }
}
```

Beschränken der "From"-Adresse

Wenn Sie eine verifizierte Domäne verwenden, können Sie eine Richtlinie erstellen, die dem stellvertretenden Sender nur ermöglicht, E-Mails von einer bestimmten E-Mail-Adresse zu senden. Um die "From"-Adresse einzuschränken, richten Sie eine Bedingung für den Schlüssel `ses: FromAddress` ein. Die folgende Richtlinie aktiviert die AWS Konto-ID 123456789012, um von der Identität zu `sendenexample.com`, aber nur von der E-Mail-Adresse `sender@example.com`.

```
{
  "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 stellvertretende Sender E-Mails senden kann

Sie können die Sendeautorisierungsrichtlinie 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 2018 eine E-Mail-Kampagne planen, können Sie mit der folgenden Richtlinie die Möglichkeit des stellvertretenden Senders, E-Mails zu versenden, auf diesen Monat beschränken.

```
{
  "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": "2018-08-31T12:00Z"
    },
    "DateLessThan": {
      "aws:CurrentTime": "2018-10-01T12:00Z"
    }
  }
}
```

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 Identitätseigentümer 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 zuzugreifen zu können, müssen Sie `SendRawEmail` auf ein Minimum.

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.

```
{
  "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-Absenders

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. Aufgrund der folgenden Richtlinie ist die AWS-Konto-ID 123456789012 in der Lage, E-Mails von der Identität example.com zu senden, allerdings nur solange der Anzeigename der "From"-Adresse auch Marketing umfasst.

```
{
  "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 AWS Konten zum Senden von sender@example.com. Wenn die „From“ (Von) -Adresse und die Feedback-Adresse beide die Domäne example.com. Die zweite Anweisung autorisiert einen IAM-Benutzer, E-Mails von sender@example.com zu senden, solange sich die E-Mail-Adresse des Empfängers unter dem example.com-Domain befindet.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuthorizeAWS",
      "Effect": "Allow",
      "Resource": "arn:aws:ses:us-east-1:999999999999:identity/sender@example.com",
      "Principal": {
        "AWS": [
          "111111111111",
          "222222222222"
        ]
      },
      "Action": [
        "SES:SendEmail",

```

```
        "SES:SendRawEmail"
    ],
    "Condition":{
        "StringLike":{
            "ses:FromAddress": "*@example.com",
            "ses:FeedbackAddress": "*@example.com"
        }
    },
    {
        "Sid": "AuthorizeInternal",
        "Effect": "Allow",
        "Resource": "arn:aws:ses:us-east-1:999999999999:identity/sender@example.com",
        "Principal": {
            "AWS": "arn:aws:iam::333333333333:user/Jane"
        },
        "Action": [
            "SES:SendEmail",
            "SES:SendRawEmail"
        ],
        "Condition": {
            "ForAllValues:StringLike": {
                "ses:Recipients": "*@example.com"
            }
        }
    }
  ]
}
```

Aufgaben des Identitätseigentümers für Amazon SES

Dieser Abschnitt beschreibt die Schritte, die Identitätseigentümer bei der Konfiguration für die Autorisierung von Sendungen durchführen müssen.

Themen

- [Bestätigen einer Identität für die Amazon SES endeautorisierung \(p. 175\)](#)
- [Einrichten der Benachrichtigungen für Identitätseigentümer Amazon SES Zusammenhang mit der \(p. 176\)](#)
- [Abrufen von Informationen vom stellvertretenden Sender für die Sendeautorisierung von Amazon SES \(p. 176\)](#)
- [Erstellen einer Richtlinie für die Amazon SES endeautorisierung \(p. 177\)](#)
- [Bereitstellen der Identitätsinformationen für den Amazon SES tenden Sender \(p. 180\)](#)
- [Verwalten Ihrer Richtlinien für die Amazon SES -Sendeautorisierung \(p. 180\)](#)

Bestätigen einer Identität für die Amazon SES endeautorisierung

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 [Verifizieren von Identitäten \(p. 52\)](#) beschrieben.

Sie können überprüfen, ob eine E-Mail-Adresse oder Domäne verifiziert ist, indem Sie den Status im Abschnitt „Identitätsverwaltung“ des [Amazon SES Konsol](#)e oder mithilfe der `GetIdentityVerificationAttributes` API-Operation

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 [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

Important

Die AWS KontenbeidesDer Identitätseigentümer und der stellvertretende Sender müssen aus der Sandbox entfernt werden, bevor eines der Konten E-Mails an nicht verifizierte Adressen senden kann.

Einrichten der Benachrichtigungen für Identitätseigentümer Amazon SES Zusammenhang mit der

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 jedoch Ihre IP-Adressen aufgrund von Nachrichten, die von einem stellvertretenden Sender gesendet wurden, auf Anti-Spam-DNS-basierten Blackhole-Listen (DNSBL) landen, kann die Zuverlässigkeit Ihrer Identitäten beschädigt werden. Aus diesem Grund sollten Sie, wenn Sie Identitätseigentümer sind, die Weiterleitung für E-Mail-Feedback für Ihre Identitäten einrichten. Weitere Informationen finden Sie unter [Per E-Mail gesendete Amazon SES S-Benachrichtigungen \(p. 289\)](#).

Stellvertretende Sender können ihre eigenen Unzustellbarkeits- und Beschwerdebenachrichtigungen für die Identitäten einrichten, für deren Verwendung sie von Ihnen autorisiert wurden. Sie können auch [Ereignisveröffentlichung \(p. 313\)](#) einrichten, um Benachrichtigungen zu senden, wenn Unzustellbarkeits- und Beschwerdeereignisse eintreten. Wenn der Identitätseigentümer die Feedback-Weiterleitung deaktiviert, muss der stellvertretende Sender Ereignisveröffentlichung einrichten, um Unzustellbarkeits- und Beschwerdeereignisse in einem Amazon SNS -Thema oder einem Kinesis Data Firehose Stream zu veröffentlichen. Wenn weder der Identitätseigentümer noch der stellvertretende Sender eine Methode zum Senden von Benachrichtigungen für Unzustellbarkeits- und Beschwerdeereignisse einrichten oder wenn der Sender den Konfigurationssatz, der die Ereignisveröffentlichung verwendet, nicht anwendet, sendet Amazon SES automatisch Ereignisbenachrichtigungen per E-Mail an die Adresse im Feld Rücksende-Das Pfadfeld der E-Mail (oder die Adresse im Feld Quelle, wenn Sie keine Adresse für den Return-Path angegeben haben), auch wenn Sie die E-Mail-Feedback-Weiterleitung deaktiviert haben. Dieser Prozess wird in der folgenden Abbildung veranschaulicht.

Abrufen von Informationen vom stellvertretenden Sender für die Sendeautorisierung von Amazon SES

Die Richtlinie für die Sendeautorisierung muss mindestens einen Prinzipal aufweisen. Dabei handelt es sich um die Entität, an die Sie die Zugriffsberechtigung erteilen. Für die Amazon SES der Sendeautorisierung kann es sich bei dem Prinzipal um ein AWS Konto, einenAWS Identity and Access Management(IAM) - Benutzer oder einen AWS -Service.

Es ist Ihnen überlassen, den Typ des Prinzipals auszuwählen. Wenn Sie jedoch über größtmögliche Kontrolle verfügen möchten, bitten Sie den stellvertretenden Sender einen IAM-Benutzer einzurichten. Auf diese Weise kann nur ein stellvertretender Sender in Ihrem Namen E-Mails senden und nicht jeder Benutzer, der sich im AWS Konto des stellvertretenden Senders befindet. Der stellvertretende Sender kann unter Einrichten eines IAM-Benutzers finden[Erstellen eines IAM-Benutzers in Ihrem AWS Konto](#)imIAM-Benutzerhandbuch.

Nachdem Sie sich entschieden haben, ob Sie einem AWS-Konto, einem IAM-Benutzer oder einem AWS-Service Zugriff gewähren möchten, bitten Sie den stellvertretenden Sender nach der AWS-Konto-ID oder dem Amazon-Ressourcenname (ARN) des IAM-Benutzers, damit Sie diese Information in Ihre Richtlinie für die Sendeautorisierung einschließen können. Sie können den stellvertretenden Sender an die Anweisungen zum Auffinden dieser Information unter [Bereitstellen von Informationen für den Identitätseigentümer \(p. 182\)](#) verweisen. Wenn der stellvertretende Sender ein AWS -Service ist, ziehen Sie die Dokumentation für diesen Service heran, um den Servicennamen zu bestimmen.

Erstellen einer Richtlinie für die Amazon SES endeautorisierung

Um einen stellvertretenden Sender zum Senden von E-Mails mit einer E-Mail-Adresse oder Domäne (einer Identität) in Ihrem Besitz zu autorisieren, erstellen Sie eine Sendeautorisierungsrichtlinie 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.

Sie können eine Richtlinie für die Sendeautorisierung auf folgende Weisen erstellen:

- Verwenden des Richtliniengenerators Mithilfe des Richtliniengenerators in der Amazon SES Konsole können Sie eine einfache Richtlinie erstellen. Zusätzlich zur Angabe, wer die E-Mails senden kann, können Sie das Versenden der E-Mails durch weitere Bedingungen einschränken. Dazu gehören die Uhrzeit und der Datumsbereich, zu dem die E-Mails gesendet werden können, die "From"-Adresse, der "From"-Anzeigenamen, die Adresse, an die Unzustellbarkeitsnachrichten und Beschwerden gesendet werden, die Empfängeradressen und die Quell-IP-Adresse. Sie können den Richtliniengenerator auch zum Erstellen einer einfachen Richtlinienstruktur verwenden und diese zu einem späteren Zeitpunkt durch das Bearbeiten der Richtlinie anpassen.
- Erstellen einer benutzerdefinierten Richtlinie— Wenn Sie erweiterte Bedingungen einschließen oder einen AWS -Service als Prinzipal verwenden möchten, können Sie eine benutzerdefinierte Richtlinie erstellen und diese mithilfe der Amazon SES-Konsole oder der Amazon SES S-API an die Identität anfügen.

In diesem Thema werden beide Methoden beschrieben.

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 stellvertretenden Sender nicht zulässt, und eine Richtlinie für sender@example.com, die den stellvertretenden Sender zulässt, kann der stellvertretende 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.

Erstellen einer Richtlinie mit dem Richtliniengenerator

Anhand des folgenden Vorgangs können Sie anhand des Richtliniengenerators eine einfache Richtlinie für die Sendeautorisierung erstellen.

So erstellen Sie eine Richtlinie mit dem Richtliniengenerator

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Identity Management entweder Domains oder Email Addresses aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie eine Richtlinie erstellen möchten.
4. Erweitern Sie im Detailbereich Identity Policies, wählen Sie Create Policy und anschließend Policy Generator aus.
5. Erstellen Sie im Assistenten eine Richtlinienanweisung, indem Sie Werte für die folgenden Felder auswählen. Weitere Informationen zu diesen Optionen finden Sie unter [Sendeautorisierungsrichtlinien \(p. 165\)](#).

- Effekt – Wenn Sie Zugriff gewähren möchten, wählen Sie Allow aus. Andernfalls wählen Sie Deny aus.
- Prinzipale— Geben Sie entweder die 12-stellige AWS Konto-ID oder den ARN eines IAM-Benutzers ein, dem Sie den Zugriff entweder erlauben oder verweigern, und wählen Sie anschließend Add. Indem Sie diesen Schritt wiederholen, können Sie weitere Prinzipale hinzufügen. Ein Beispiel für eine AWS Konto-ID ist 1234589012 und ein Beispiel für einen IAM-Benutzer-ARN ist `arn:aws:iam#123456789012:user/John`.

Note

Der Assistent des Richtliniengenerators unterstützt derzeit keine AWS-Service-Prinzipale. Um einen AWS -Serviceprinzipal hinzuzufügen, müssen Sie entweder [Erstellen einer benutzerdefinierten Richtlinie \(p. 179\)](#) oder verwenden Sie den Richtliniengenerator, um ein AWS Konto oder einen IAM-Benutzerprinzipal hinzuzufügen, und anschließend [Bearbeiten von \(p. 180\)](#) die Politik.

- Aktionen— Wählen Sie den Zugriff auf die E-Mail-Sendefunktionen, auf die diese Richtlinie zutrifft. In der Regel wählen Identitätseigentümer beide Optionen, um dem stellvertretenden Sender die Wahl zu überlassen, wie die E-Mails gesendet werden sollen. Weitere Informationen finden Sie unter [Richtlinienspezifische Anweisungen \(p. 167\)](#).
6. (Optional) Wenn Sie der Richtlinie Einschränkungen hinzufügen möchten, klicken Sie auf Add Conditions und wählen Sie anschließend die folgenden Informationen aus:
- Schlüssel— Hierbei handelt es sich um das besondere Merkmal, das die Grundlage für die Zugriffsbeschränkung bildet. Über den Richtliniengenerator können Sie einen speziellen Amazon SES -Schlüssel oder ein paar häufig genutzte AWS-weite Schlüssel (aktuelle Zeit und Quell-IP) auswählen. Details dazu finden Sie unter [Conditions \(p. 168\)](#). Wenn Sie die erweiterten AWS-weiten Schlüssel, die unter [Verfügbare Schlüssel](#) aufgelistet sind, auswählen möchten, können Sie die Richtlinie zunächst erstellen und anschließend entsprechend bearbeiten.
 - Bedingung— Dies ist der Bedingungstyp, den Sie festlegen möchten. Beispielsweise gibt es Bedingungen im Zusammenhang mit Zeichenfolgen, mit numerischen Werten, dem Datum und der Uhrzeit usw. Eine Liste der Bedingungen finden Sie unter [Bedingungstypen](#) im IAM-Benutzerhandbuch.
 - Value— Dieser Wert wird gegen die Bedingung getestet. Beispiele finden Sie in den Richtlinien unter [Beispiele von Sendeautorisierungsrichtlinien \(p. 170\)](#).

Nachdem Sie den Schlüssel, die Bedingung und den Wert ausgewählt haben, wählen Sie Add Condition aus. Die Bedingung wird in der Liste mit den Conditions angezeigt. Um eine Bedingung zu entfernen, klicken Sie in der Liste neben der Bedingung auf Remove. Wenn Sie eine andere Bedingung hinzuzufügen möchten, wählen Sie Add Conditions aus.

The screenshot shows the 'Policy Generator' tool in the Amazon SES console. It is designed to help users create a basic sending authorization policy by generating simple statements. The interface includes the following fields and options:

- Identity:** A text field containing 'example.com'.
- Effect:** Radio buttons for 'Allow' (selected) and 'Deny'.
- Principals*:** A text field containing '123456789012'.
- Actions*:** Checkboxes for 'ses:SendEmail' and 'ses:SendRawEmail', both of which are checked.
- Conditions:** A section titled 'Add Conditions (optional)' containing a form with:
 - Key:** A dropdown menu set to 'ses:FromAddress'.
 - Condition:** A dropdown menu set to 'StringEquals'.
 - Value:** A text field containing 'marketing@example.com'.
 - Add Condition:** A button to add the configured condition to the list.
- Buttons:** At the bottom, there is an 'Add Statement' button, and at the bottom right, 'Cancel' and 'Next' buttons.

Below the 'Actions' section, a note states: 'Fields marked with asterisk (*) are required.'

7. Klicken Sie nach dem Hinzufügen von Bedingungen auf Add Statement. Die Anweisung wird in der Liste Statements angezeigt, wo Sie sie bearbeiten oder entfernen können. Sie können zusätzliche Anweisungen hinzufügen, indem Sie die Schritte 5 bis 7 wiederholen.
8. Wenn Sie alle Anweisungen hinzugefügt haben, wählen Sie Next aus.
9. Überprüfen Sie die Richtlinie im Dialogfeld Edit Policy, bearbeiten Sie sie bei Bedarf und klicken Sie anschließend auf Apply Policy.

Erstellen einer benutzerdefinierten Richtlinie

Wenn Sie eine benutzerdefinierte Richtlinie erstellen und Sie einer Identität anfügen möchten, haben Sie die folgenden Optionen:

- Verwenden der Amazon SES API— Erstellen Sie die Richtlinie in einem Texteditor und fügen Sie sie anschließend der Identität, wie Sie mithilfe der `PutIdentityPolicy` API, die in der [Amazon Simple Email Service API-Referenz](#).
- Verwenden 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 mithilfe des Editors für benutzerdefinierte Richtlinien

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Identity Management entweder Domains oder Email Addresses aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie eine Richtlinie erstellen möchten.
4. Erweitern Sie im Detailbereich die Option Identity Policies, wählen Sie Create Policy und anschließend Custom Policy aus.
5. Fügen Sie im Bereich Edit Policy den Text Ihrer Richtlinie ein.
6. Klicken Sie auf Apply Policy.

Bereitstellen der Identitätsinformationen für den Amazon SES tenden Sender

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. Wenden Sie das folgende Verfahren an, um den ARN Ihrer Identität zu finden.

So finden Sie den ARN einer Identität

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Identity Management entweder Domains oder Email Addresses aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, der Sie die Sendeautorisierungsrichtlinie angefügt haben.
4. Der Identitäts-ARN wird oben im Detailbereich nach Identity ARN angezeigt. 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.

Verwalten Ihrer Richtlinien für die Amazon SES - Sendeautorisierung

Zusätzlich zum Erstellen und Anfügen von Richtlinien an Identitäten wie unter [Erstellen einer Richtlinie](#) (p. 177) beschrieben, können Sie die Richtlinien einer Identität auch bearbeiten, entfernen auflisten und abrufen, wie in den folgenden Abschnitten erklärt.

Note

Um Berechtigungen zu widerrufen, können Sie eine Richtlinie entweder bearbeiten oder entfernen.

Bearbeiten einer Richtlinie

Der einfachste Weg, eine Richtlinie zu bearbeiten, erfolgt über die Verwendung der Amazon SES Konsole. Wenn Sie stattdessen die Amazon SES API verwenden möchten, können Sie die [GetIdentityPolicies](#) Verwenden Sie dann die Richtlinie mithilfe eines Texteditors, um die Richtlinie abzurufen, anhand eines Texteditors bearbeiten und anschließend die [PutIdentityPolicy](#), um die ältere Richtlinie zu überschreiben.

Im folgenden Abschnitt erfahren Sie, wie Sie eine Richtlinie mit der Amazon SES Konsole bearbeiten.

So bearbeiten Sie eine Richtlinie mithilfe der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Identity Management entweder Domains oder Email Addresses aus.
3. Klicken Sie in der Liste der Identitäten auf die Identität, die der Richtlinie, die Sie bearbeiten möchten, zugeordnet ist.
4. Erweitern Sie im Detailbereich die Option Identity Policies.
5. Wählen Sie Edit Policy neben der Richtlinie aus, die Sie ändern möchten.
6. Bearbeiten Sie die Richtlinie im Bereich Edit Policy und wählen Sie anschließend Apply Policy aus.
7. Klicken Sie im Dialogfeld Overwrite Existing Policy auf Overwrite.

Entfernen einer Richtlinie

Um eine Berechtigungen aufzuheben, können Sie die Richtlinie jederzeit einfach entfernen. Sie können eine Richtlinie mithilfe der [DeleteIdentityPolicy](#) oder Sie können die Amazon SES Konsole verwenden, wie im folgenden Verfahren dargestellt.

Important

Nachdem Sie eine Richtlinie entfernt haben, gibt es keine Möglichkeit, sie wiederherzustellen. Wir empfehlen, die Richtlinie vor dem Entfernen durch Kopieren und Einfügen in eine Textdatei zu sichern.

So entfernen Sie eine Richtlinie mithilfe der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Identity Management entweder Domains oder Email Addresses aus.
3. Klicken Sie in der Liste der Identitäten auf die Identität, die der Richtlinie, die Sie entfernen möchten, zugeordnet ist.
4. Erweitern Sie im Detailbereich die Option Identity Policies. Wählen Sie Remove Policy neben der Richtlinie aus, die Sie entfernen möchten.
5. Wählen Sie im Dialogfeld Remove Policy die Option Yes, Remove Policy aus.

Auflisten und Abrufen von Richtlinien

Sie können die Richtlinien, die mit einer Identität verknüpft sind, mithilfe der [ListIdentityPolicies](#)-API-Operation auflisten. Sie können auch die Richtlinien selbst mithilfe der [GetIdentityPolicies](#)-API-Operation abrufen.

Sie können auch die Amazon SES Konsole verwenden, um beide Aufgaben auszuführen, wie im folgenden Verfahren beschrieben.

So können Sie mithilfe der Amazon SES Konsole die Richtlinien auflisten und anzeigen, die einer Identität zugeordnet sind

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Identity Management entweder Domains oder Email Addresses aus.
3. Wählen Sie in der Liste der Identitäten die Identität aus, für die Sie Richtlinien anzeigen möchten.

4. Erweitern Sie im Detailbereich die Option Identity Policies.
5. Wählen Sie Show Policy neben der Richtlinie aus, die Sie anzeigen möchten.

Delegieren der Senderaufgaben für die Amazon SES endeautorisierung

Als stellvertretender Sender schicken Sie kontoübergreifende E-Mails. Das bedeutet, dass Sie im Namen einer Identität, deren Eigentümer Sie nicht sind, aber für deren Nutzung Sie autorisiert sind, E-Mails versenden. Auch wenn Sie die E-Mails im Namen des Identitätseigentümers versenden, werden die Unzustellbarkeitsnachrichten und Beschwerden den Unzustellbarkeits- und Beschwerdemetriken Ihres AWS Kontos angerechnet und die Anzahl der gesendeten Nachrichten wirkt sich auf Ihre Sendequote aus. Sie sind auch dafür verantwortlich, wenn Sie eine Erhöhung des Sendekontingents anfordern, um die E-Mails des Identitätseigentümers zu versenden.

Als stellvertretender Sender müssen Sie die folgenden Aufgaben ausführen:

- [Bereitstellen von Informationen für den Identitätseigentümer \(p. 182\)](#)
- [Benachrichtigungen an den stellvertretenden Sender \(p. 182\)](#)
- [Senden von E-Mails im Namen des Identitätseigentümers \(p. 185\)](#)

Bereitstellen von Informationen für den Identitätseigentümer der Amazon SES endeautorisierung

Als stellvertretender Sender müssen Sie dem Identitätseigentümer Ihre AWS Konto-ID oder den Amazon-Ressourcennamen (ARN) des AWS Identity and Access Management (IAM) -Benutzers, der eine E-Mail im Namen des Identitätseigentümers sendet. Sie finden diese Informationen durch das folgende Verfahren.

So suchen Sie Ihre AWS-Konto-ID

1. Melden Sie sich beim AWS Management Console an <https://console.aws.amazon.com>.
2. Wählen Sie im Navigationsmenü Ihren Namen aus und klicken Sie dann auf My Account.
3. Erweitern Sie Account Settings. In diesem Abschnitt wird Ihre AWS Konto-ID angezeigt.

So finden Sie den ARN eines IAM-Benutzers

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Management-Konsole unter <https://console.aws.amazon.com/iam/>.
2. Klicken Sie im Navigationsbereich auf Users.
3. Wählen Sie in der Liste der Benutzer den Namen des Benutzers aus. Der Bereich Summary zeigt den ARN an. Der ARN sieht in etwa wie folgendes Beispiel aus: `arn:aws:iam::123456789012:user/John`.

Benachrichtigungen an stellvertretende Sender bei Verwendung der Amazon SES endeautorisierung

Als stellvertretender Sender werden Unzustellbarkeits- und Beschwerdenachrichten Ihren Unzustellbarkeits- und Beschwerdemetriken angerechnet, nicht denen des Identitätseigentümers. Wenn die Unzustellbarkeits- oder Beschwerdequoten für Ihr Konto zu hoch wird, legen wir möglicherweise eine Prüfung für Ihr Konto fest oder unterbrechen die Fähigkeit Ihres Kontos zum Versenden von E-Mails. 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.

Stellvertretende Sender können Amazon SES so einrichten, dass Benachrichtigungen gesendet werden, wenn Unzustellbarkeits- und Beschwerdeereignisse eintreten. Absender von Delegaten können auch [Ereignisveröffentlichung](#) (p. 313) Um Unzustellbarkeits- und Beschwerdebenachrichtigungen für Amazon SNS oder Kinesis Data Firehose zu veröffentlichen.

Note

Wenn Sie Amazon SES zum Senden von Benachrichtigungen über Amazon SNS einrichten, werden Ihnen die üblichen Amazon SNS-Standardgebühren für die Benachrichtigungen, die Sie erhalten, berechnet. Weitere Informationen finden Sie im [Amazon SNS Preise](#).

Themen

- [Einrichten einer kontoübergreifenden Amazon SES Identitätsbenachrichtigung](#) (p. 183)
- [Bearbeiten einer kontoübergreifenden Amazon SES S-Benachrichtigungskonfiguration](#) (p. 184)
- [Anzeigen Ihrer kontoAmazon SES -Identitätsbenachrichtigungen für](#) (p. 184)
- [Entfernen einer kontoübergreifenden Amazon SES S-Identität](#) (p. 185)

Einrichten einer kontoübergreifenden Amazon SES Identitätsbenachrichtigung

Bevor Sie die Benachrichtigungen einrichten können, benötigen Sie den Amazon-Ressourcenname (ARN) der Identität, für deren Nutzung Sie der Identitätseigentümer autorisiert hat und für die Sie Benachrichtigungen konfigurieren möchten. Der ARN für die Identität `user@example.com` ähnelt beispielsweise dem folgenden Beispiel: `arn:aws:ses:us-east-1:123456789012:identity/user@example.com`. Wenn der Identitätseigentümer Ihnen den ARN der Identität noch nicht gegeben hat, verweisen Sie ihn an den Vorgang unter [Bereitstellen der Identitätsinformationen für den stellvertretenden Sender](#) (p. 180).

Der einfachste Weg, eine Benachrichtigung zu konfigurieren, erfolgt über die Amazon SES Konsole. Verwenden Sie die API-Operation [SetIdentityNotificationTopic](#), um den ARN des Identitätseigentümers als `Identity`-Parameter zu übergeben.

Im folgenden Abschnitt erfahren Sie, wie Sie Benachrichtigungen mit der Amazon SES Konsole einrichten.

So richten Sie -UnAmazon SNS stellbarkeits-, Beschwerde- oder Zustellbenachrichtigungen über die Amazon SES -Konsole ein

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich Cross-Account Notifications (Kontoübergreifende Benachrichtigungen) aus.
3. Wählen Sie Add Notification Config aus.
4. Geben Sie im Dialogfeld Add Notification Configuration (Benachrichtigungskonfiguration hinzufügen) für Identity ARN (Identitäts-ARN) den ARN der Identität ein, für die Sie Benachrichtigungen konfigurieren möchten. Die Identität darf nicht dem Konto zugeordnet sein, bei dem Sie derzeit angemeldet sind.
5. Wählen Sie die Amazon SNS -Themen aus, die für Unzustellbarkeitsnachrichten, Beschwerden oder Zustellungen verwendet werden sollen. Sie können auch neue Amazon SNS Themen für diese Benachrichtigungen erstellen.

Important

Die Amazon SNS -Themen, die Sie für Amazon SES S-Benachrichtigungen verwenden möchten, müssen der gleichen AWS Region angehören, die Sie für das Senden von E-Mails mit Amazon SES verwenden.

Sie können wählen, ob die Unzustellbarkeits-, Beschwerde- und Zustellbenachrichtigungen im gleichen Amazon SNS-Thema oder in verschiedenen Amazon SNS-Themen veröffentlicht werden sollen. Wenn Sie ein Amazon SNS -Thema verwenden möchten, dessen Eigentümer Sie nicht sind, muss der Eigentümer des Themas eine Amazon SNS-Zugriffsrichtlinie konfigurieren, die Sie berechtigt, die `SNS:Publish`-Aktion zu ihrem Thema. Weitere Informationen darüber, wie Sie den Zugriff auf Ihr Amazon SNS Thema mithilfe von IAM-Richtlinien kontrollieren, finden Sie unter [Verwalten des Zugriffs auf Ihre Amazon SNS -Themen](#).

6. Wählen Sie **Save Config**, um die Benachrichtigungskonfiguration zu speichern. Es kann einige Zeit dauern, bis die Änderungen angewendet werden.

Bearbeiten einer kontenübergreifenden Amazon SES S-Benachrichtigungskonfiguration

Der einfachste Weg, eine Benachrichtigungskonfiguration zu bearbeiten, erfolgt über die Amazon SES Konsole. Wenn Sie stattdessen die Amazon SES API verwenden möchten, können Sie die `SetIdentityNotificationTopic`-API-Operation und übergeben Sie den ARN der Identität als `Identity`-Parameter.

Im folgenden Abschnitt erfahren Sie, wie Sie eine kontoübergreifende Benachrichtigungskonfiguration mithilfe der Amazon SES -Konsole bearbeiten.

So bearbeiten Sie eine kontoübergreifende Benachrichtigungskonfiguration mithilfe der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich **Cross-Account Notifications** aus.

Im Detailbereich **Cross-Account Notifications** finden Sie alle kontoübergreifenden Identitäten, für die Sie Benachrichtigungen eingerichtet haben.

3. Wählen Sie den ARN der Identität aus, für die Sie die Benachrichtigungskonfiguration anzeigen möchten.
4. Bearbeiten Sie die Benachrichtigungseinstellungen und wählen Sie anschließend **Save Config** aus.

Anzeigen Ihrer kontenAmazon SES -Identitätsbenachrichtigungen für

Der einfachste Weg, eine Benachrichtigungskonfiguration anzuzeigen, erfolgt über die Amazon SES Konsole. Verwenden Sie die API-Operation `GetIdentityNotificationAttributes`, um den ARN der Identität als `Identity`-Parameter zu übergeben.

Note

Die einzigen kontoübergreifenden Identitäten, die in der Liste der kontoübergreifenden Identitäten angezeigt werden, sind die Identitäten, für die Sie Benachrichtigungen mithilfe des unter [Einrichten einer Benachrichtigungskonfiguration](#) (p. 183) beschriebenen Verfahrens konfiguriert haben.

So zeigen Sie die kontoübergreifenden Benachrichtigungskonfigurationen mithilfe der Amazon SES Konsole an

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich **Cross-Account Notifications** aus.

Im Detailbereich **Cross-Account Notifications** finden Sie alle kontoübergreifenden Identitäten, für die Sie Benachrichtigungen eingerichtet haben.

3. Wählen Sie den ARN einer Identität aus.

Das Dialogfeld Edit Configuration Notification zeigt die Einstellungen der Identität an.

Entfernen einer kontoübergreifenden Amazon SES S-Identität

Der einfachste Weg, eine Benachrichtigungskonfiguration zu entfernen, erfolgt über die Amazon SES Konsole. Verwenden Sie die API-Operation [SetIdentityNotificationTopic](#), um den ARN des Identitätseigentümers als `Identity`-Parameter und Null für den `SnsTopic`-Parameter zu übergeben. Um die Benachrichtigungskonfiguration vollständig zu entfernen, müssen Sie diesen Vorgang für jeden eingerichteten Benachrichtigungstyp (Unzustellbarkeit, Beschwerde und Zustellung) durchführen.

Note

Wenn Sie eine Benachrichtigungskonfiguration entfernen, wird der ARN der kontoübergreifenden Identität aus der Liste der kontoübergreifenden Identitäts-ARNs in der Amazon SES S-Konsole entfernt. Dies bedeutet nicht, dass Sie nicht weiterhin E-Mails für diese Identität senden können. Es bedeutet lediglich, dass Sie hierfür nicht länger Unzustellbarkeits-, Beschwerde- und Zustellbenachrichtigungen erhalten werden. Wenn Sie die Benachrichtigungen erneut aktivieren möchten, müssen Sie nur den Einrichtungsvorgang für die Benachrichtigungen wiederholen, wie unter [Einrichten einer Benachrichtigungskonfiguration](#) (p. 183) beschrieben.

Im folgenden Abschnitt erfahren Sie, wie Sie eine kontoübergreifende Benachrichtigungskonfiguration mithilfe der Amazon SES -Konsole entfernen.

So entfernen Sie eine kontoübergreifende Benachrichtigungskonfiguration mithilfe der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich Cross-Account Notifications aus.

Im Detailbereich Cross-Account Notifications finden Sie alle kontoübergreifenden Identitäten, für die Sie Benachrichtigungen eingerichtet haben.

3. Wählen Sie das Feld links neben der Identität aus, die Sie entfernen möchten, und klicken Sie anschließend auf Remove.
4. Wählen Sie im Dialogfeld Remove Cross-Account Notification Config die Option Delete Notification config aus.

Der ARN der kontoübergreifenden Identität wird aus der Liste der kontoübergreifenden Identitäts-ARNs entfernt. Dies bedeutet nicht, dass Sie für die Identität keine E-Mails mehr senden können, sondern nur, dass Sie für diese Identität keine Benachrichtigungen mehr erhalten.

Senden von E-Mails im Namen des Identitätseigentümers für die Amazon SES

Als stellvertretender Sender senden Sie E-Mails wie jeder andere Amazon SES Sender auch, mit der Ausnahme, dass Sie den ARN der Identität angeben, für deren Nutzung Sie vom Identitätseigentümer 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 mit dem Amazon SES S-Endpunkt in der AWS Region herstellen, in der der Identitätseigentümer die Identität verifiziert hat. Darüber hinaus werden die AWS Konten von beides Der Identitätseigentümer und der stellvertretende Sender müssen aus der Sandbox entfernt werden, bevor eines der Konten E-Mails an nicht verifizierte Adressen senden kann. Weitere Informationen finden Sie unter [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

Verwenden der Amazon SES API

Wie alle E-Mail-Sender von Amazon SES, die auf Amazon SES über die Amazon SES -API zugreifen (entweder direkt über HTTPS oder indirekt durch ein AWS S-SDK), können Sie sich für eine von zwei Aktionen zum Senden von E-Mails entscheiden: `SendEmail` und `SendRawEmail`. Die [Amazon Simple Email Service API-Referenz](#) beschreibt die Details dieser APIs, allerdings finden Sie hier eine Übersicht über die Parameter für die Sendeautorisierung.

SendRawEmail

Wenn Sie `SendRawEmail` verwenden möchten, um das Format Ihrer E-Mails kontrollieren zu können, können Sie die kontoübergreifende 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	Beschreibung
<code>SourceArn</code>	ARN der Identität, die mit der Sendeautorisierungsrichtlinie verknüpft ist, die Sie zum Senden von E-Mail im Namen der im <code>Source</code> -Parameter von <code>SendRawEmail</code> angegebenen E-Mail-Adresse berechtigt. Note Wenn Sie nur die <code>SourceArn</code> festgelegt, gibt Amazon SES für die Adressen „From“ und „Return Path“ die Identität an, die Sie im <code>SourceArn</code> .
<code>FromArn</code>	ARN der Identität, die mit der Sendeautorisierungsrichtlinie verknüpft ist, die Sie zur Angabe einer bestimmten "From"-Adresse im Header der Raw-E-Mail-Adresse berechtigt.
<code>ReturnPathArn</code>	ARN der Identität, die mit der Sendeautorisierungsrichtlinie verknüpft ist, die Sie zum Verwenden der im <code>ReturnPath</code> -Parameter von <code>SendRawEmail</code> 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 "From", "Reply-to" oder "Subject") 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	Beschreibung
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-west-2:123456789012:identity/example.com
X-SES-FROM-ARN: arn:aws:ses:us-west-2:123456789012:identity/example.com
X-SES-RETURN-PATH-ARN: arn:aws:ses:us-west-2:123456789012: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

Wenn Sie die Operation `SendEmail` verwenden, können Sie die kontoübergreifende Identität angeben, indem Sie die nachfolgenden optionalen Parameter übergeben. Für die Methode `SendEmail` können Sie nicht die X-Header-Methode verwenden.

Parameter	Beschreibung
SourceArn	ARN der Identität, die mit der Sendeautorisierungsrichtlinie verknüpft ist, die Sie zum Senden von E-Mail im Namen der im Source-Parameter von <code>SendRawEmail</code> angegebenen E-Mail-Adresse berechtigt.
ReturnPathArn	ARN der Identität, die mit der Sendeautorisierungsrichtlinie verknüpft ist, die Sie zum Verwenden der im ReturnPath-Parameter von <code>SendRawEmail</code> angegebenen E-Mail-Adresse berechtigt.

Das folgende Beispiel zeigt, wie Sie eine E-Mail mit dem `SourceArn` und `ReturnPathArn`-Attribute verwenden `SendEmail`-Operation und die Berechtigung [SDK für Python](#).

```
import boto3
from botocore.exceptions import ClientError

# Create a new SES resource and specify a region.
client = boto3.client('ses', region_name="us-west-2")

# 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-west-2:123456789012:identity/example.com',
        ReturnPathArn='arn:aws:ses:us-west-2:123456789012: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 SMTP-Schnittstelle von Amazon SES

Wenn Sie die -SMTP-Schnittstelle von Amazon SES für das kontoübergreifende Senden verwenden, müssen Sie die `X-SES-SOURCE-ARN`, `X-SES-FROM-ARN` und `X-SES-RETURN-PATH-ARN`-Header in Ihrer Nachricht. Übergeben Sie diese Header, nachdem Sie den `DATA`-Befehl in der SMTP-Aushandlung erteilen.

Verwenden dedizierter IP-Adressen mit Amazon SES

Wenn Sie ein neues Amazon SES-Konto erstellen, werden Ihre E-Mails von IP-Adressen gesendet, die mit anderen Amazon SES-Benutzern geteilt werden. Gegen [eine zusätzliche monatliche Gebühr](#) können Sie dedizierte IP-Adressen mieten, die für Ihre ausschließliche Nutzung reserviert sind. Beide Optionen bieten einzigartige Vor- und Nachteile, die in der folgenden Tabelle zusammengefasst sind. Klicken Sie auf einen Punkt in der Spalte Vorteil, um weitere Informationen zu diesem Vorteil zu erhalten.

Vorteil	Gemeinsame IP-Adressen	Dedizierte IP-Adressen
Sofort einsatzbereit ohne zusätzliches Setup (p. 189)	Ja	Nein
Zuverlässigkeit durch AWS verwaltet (p. 190)	Ja	Nein
Geeignet für Kunden mit kontinuierlichen, planbaren Versandmustern (p. 190)	Ja	Ja
Geeignet für Kunden mit weniger planbaren Versandmustern (p. 190)	Ja	Nein
Geeignet für Versender von großen Volumen (p. 190)	Ja	Ja
Geeignet für Versender von geringem Volumen (p. 190)	Ja	Nein
Zusätzliche monatliche Kosten (p. 190)	Nein	Ja
Vollständige Kontrolle über die Reputation des Absenders (p. 191)	Nein	Ja
Isolierung der Reputation nach E-Mail-Typ, Empfänger oder anderen Faktoren (p. 191)	Nein	Ja
Stellt bekannte IP-Adressen zur Verfügung, die sich nie ändern. (p. 191)	Nein	Ja

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 dedizierte IP-Adressen in Fällen verwenden, in denen Sie nur geringe Mengen an E-Mails versenden, oder wenn Ihre Versandmuster sehr unregelmäßig sind, können Zustellbarkeitsprobleme auftreten.

Einfache Einrichtung

Wenn Sie sich dafür entscheiden, gemeinsam genutzte IP-Adressen zu verwenden, müssen Sie keine zusätzliche Konfiguration vornehmen. Ihr Amazon SES Konto kann E-Mails senden, sobald Sie eine E-Mail-Adresse verifizieren und aus der Sandbox verschieben.

Wenn Sie dedizierte IP-Adressen mieten möchten, müssen Sie [eine Anfrage senden \(p. 191\)](#) und optional [dedizierte IP-Pools konfigurieren \(p. 196\)](#).

Zuverlässigkeit durch AWS

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.

Freigegebene IP-Adressen werden von mehreren Amazon SES Kunden gemeinsam verwendet. Diese Kunden senden zusammen eine große Menge von E-Mails. Dieser ausgehende Datenverkehr wird sorgfältig verwaltet, um die Zuverlässigkeit der gemeinsam genutzten IP-Adressen zu maximieren.

Wenn Sie dedizierte IP-Adressen verwenden, liegt es in Ihrer Verantwortung, Ihre Reputation als Absender aufrechtzuerhalten, indem Sie konsistente und vorhersehbare Mengen an E-Mails versenden.

Note

Wenn Sie Smart Network Data Services (SNDS) Daten für Ihre dedizierten IPs anzeigen möchten, lesen Sie [SNDS-Metriken für dedizierte IP-Adressen](#) (p. 418). Weitere Informationen finden Sie unter.

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.

Wenn Ihre E-Mail-Versandmuster unregelmäßig sind (das heißt, sie folgen keinem planbaren Muster), dann sind die freigegebenen IP-Adressen wahrscheinlich besser auf Ihre Bedürfnisse zugeschnitten. Wenn Sie gemeinsam genutzte IP-Adressen verwenden, können Sie Ihre E-Mail-Versandmuster entsprechend der Situation erhöhen oder verringern.

Wenn Sie dedizierte IP-Adressen verwenden, müssen Sie diese Adressen "einführen", indem Sie die Menge der versendeten E-Mails mit jedem Tag erhöhen. Der Prozess der "Einführung" neuer IP-Adressen ist in [Aufwärmen dedizierter IP-Adressen](#) (p. 194) beschrieben. Sobald Ihre dedizierten IP-Adressen eingeführt sind, müssen Sie ein konsistentes Sendeverhalten beibehalten.

Volumen ausgehender E-Mails

Dedizierte IP-Adressen eignen sich am besten für Kunden, die große Mengen an E-Mails versenden. Die meisten Internetdienstanbieter (ISPs) verfolgen die Reputation einer bestimmten IP-Adresse nur dann, wenn sie von dieser Adresse aus eine beträchtliche Menge an E-Mails 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 Sie unter Umständen dedizierte IP-Adressen verwenden, wenn Sie keine großen Mengen an E-Mails versenden. Beispielsweise können dedizierte IP-Adressen 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

Die Verwendung von gemeinsam genutzten IP-Adressen ist im normalen -Preis von Amazon SES inbegriffen. Das Mieten von dedizierten IP-Adressen verursacht zusätzliche monatliche Kosten, die über die Standardkosten für den Versand von E-Mails über Amazon SES hinausgehen. Für jede dedizierte IP-Adresse wird eine separate monatliche Gebühr erhoben. Informationen zu den Preisen finden Sie unter [Amazon SES — Preise](#).

Kontrolle über die Senderreputation

Wenn Sie dedizierte IP-Adressen verwenden, ist Ihr Amazon SES -Konto das einzige, das in der Lage ist, E-Mails von diesen Adressen aus zu versenden. Aus diesem Grund wird die Reputation des Absenders der von Ihnen gemieteten dedizierten IP-Adressen durch Ihre E-Mail-Versandpraktiken bestimmt.

Möglichkeit zur Isolierung der Reputation des Absenders

Indem Sie dedizierte IP-Adressen verwenden, können Sie Ihre Absenderreputation für verschiedene Elemente Ihres E-Mail-Programms isolieren. Wenn Sie mehr als eine dedizierte IP-Adresse für die Verwendung mit Amazon SES mieten, können Sie **Dedicated IP-Pools**— 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. Weitere Informationen hierzu finden Sie unter [Erstellen von dedizierten IP-Pools](#) (p. 196).

Bekannte, unveränderliche IP-Adressen

Wenn Sie dedizierte IP-Adressen verwenden, finden Sie die Werte der Adressen, über die Ihre E-Mails gesendet werden, im Abschnitt **Dedizierte IPs** der Amazon SES Konsole. Dedizierte IP-Adressen ändern sich nicht.

Bei gemeinsam genutzten IP-Adressen kennen Sie die von Amazon SES zum Versenden Ihrer E-Mails verwendeten IP-Adressen nicht. Sie können sich jederzeit ändern.

Beantragen und Freisetzen von dedizierten IP-Adressen

In diesem Abschnitt wird beschrieben, wie Sie dedizierte IP-Adressen anfordern bzw. freigeben, indem Sie eine entsprechende Anforderung an das [AWS Supportzentrum](#) senden. Wir berechnen Ihrem Konto für jede dedizierte IP-Adresse, die Sie für Amazon SES leasen, eine zusätzliche monatliche Gebühr. Weitere Informationen zu den Kosten für dedizierte IP-Adressen finden Sie unter [Amazon SES – Preise](#).

Bewährte Methoden für die Arbeit mit IP-Adressen

Auch wenn es kein Mindestkontingent gibt, sollten Sie mehr als eine dedizierte IP-Adresse in jeder AWS Region leasen, in der Sie Amazon SES verwenden. Jede AWS Region besteht aus mehreren physischen Standorten, den **Availability Zones**. Wenn Sie mehr als eine dedizierte IP-Adresse leasen, verteilen wir diese Adressen so gleichmäßig wie möglich über die Availability Zones in der AWS Region, die Sie in Ihrer Anfrage angegeben haben. Wenn Sie Ihre dedizierten IP-Adressen auf diese Weise über Availability Zones verteilen, werden dadurch die Verfügbarkeit und Redundanz Ihrer dedizierten IP-Adressen erhöht.

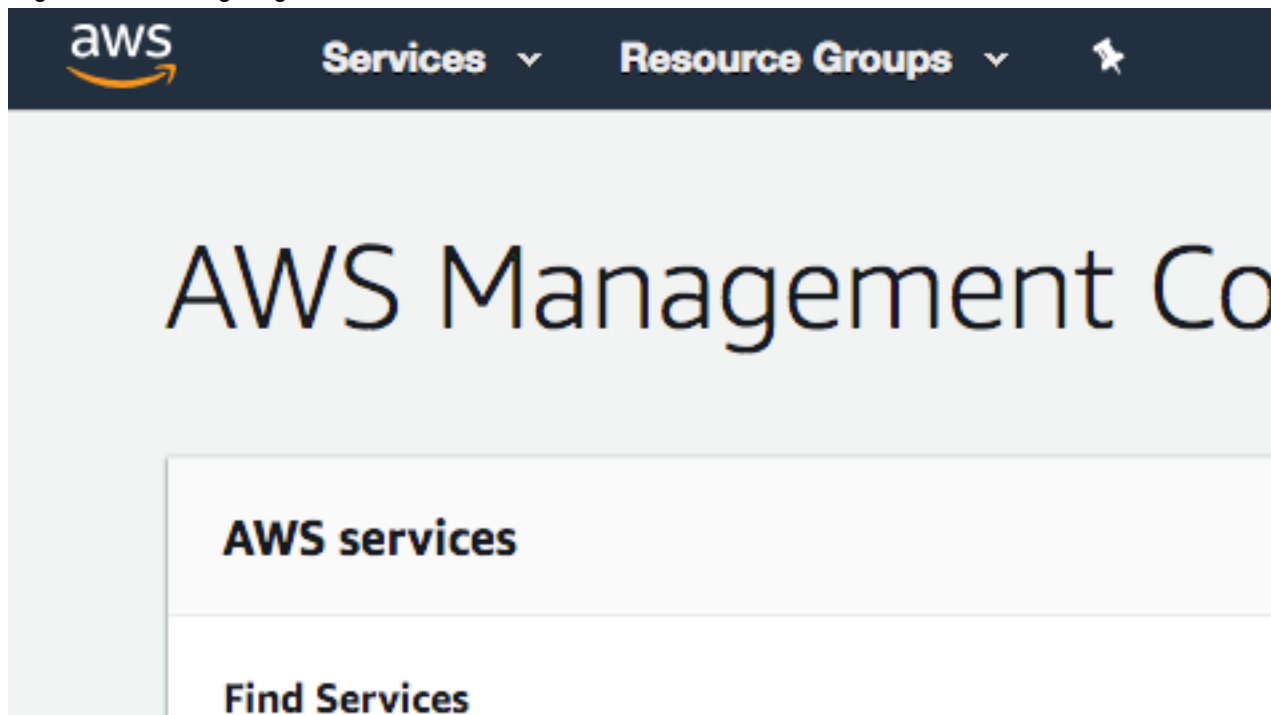
Eine Liste aller Regionen, in denen Amazon SES derzeit verfügbar ist, finden Sie unter [AWS-Regionen und -Endpunkte](#) im Allgemeinen Amazon Web Services Referenz. Weitere Informationen über die in jeder Region verfügbare Anzahl von Availability Zones finden Sie unter [Globale AWS-Infrastruktur](#).

Beantragen dedizierter IP-Adressen

In den folgenden Schritten wird beschrieben, wie Sie dedizierte IP-Adressen anfordern, indem Sie im AWS Support Center einen Fall zur Erhöhung des Sendekontingents erstellen. Mit diesem Verfahren können Sie so viele dedizierte IP-Adressen beantragen, wie Sie benötigen.

So beantragen Sie dedizierte IP-Adressen

1. Melden Sie sich beim an.AWS Management Consoleum<https://console.aws.amazon.com/>.
2. Wählen Sie im Menü Support (Support) die Option Support Center (Support-Center) aus, wie in der folgenden Abbildung dargestellt.



3. Wählen Sie Create case (Fall erstellen) aus.
4. Wählen Sie unter Create case (Fall erstellen) die Option Service limit increase (Erhöhung des Service Limits) aus.
5. Führen Sie unter Case classification (Fallklassifizierung) die folgenden Abschnitte aus:
 - Wählen Sie für Limit Type (Limit-Typ) die Option SES Sending Limits (SES-Sendelimits) aus.
 - Geben Sie als Mail Type (E-Mail-Typ) an, welche Art von E-Mail Sie mit der dedizierten IP-Adresse senden möchten. Wenn mehrere Werte zutreffen, wählen Sie die Option aus, die für die meisten der E-Mails gelten, die Sie senden möchten.
 - Geben Sie als Website URL (Website-URL) die URL der Website ein. Durch die Bereitstellung dieser Informationen können wir besser einschätzen, welche Art von Inhalt Sie senden möchten.
 - Für Meine E-Mail-Sendefunktionen entsprechen den AWS -Servicebedingungen und AUPWählen Sie die Option aus, die Ihrem Anwendungsfall entspricht.
 - Wählen Sie unter I only send to recipients who have specifically requested my mail (Ich sende nur an Empfänger, die meine Mail explizit angefordert haben) die Option aus, die Ihrem Anwendungsfall entspricht.
 - Wählen Sie unter I have a process to handle bounces and complaints (Ich habe einen Prozess für die Verarbeitung von unzustellbaren E-Mails und Beschwerden) die Option aus, die Ihrem Anwendungsfall entspricht.
6. Führen Sie unter Requests (Anforderungen) die folgenden Abschnitte aus:
 - FürRegionWählen Sie die AWS Region aus, für die Ihre Anfrage gilt.
 - Wählen Sie als Limit die Option Desired Maximum Send Rate (Gewünschte maximale Senderate) aus.

- Geben Sie als New limit value (Neuer Limit-Wert) die maximale Anzahl der Nachrichten ein, die Sie pro Sekunde senden müssen. Wir verwenden den Wert, den Sie angeben, um die Anzahl der dedizierten IP-Adressen zu berechnen, die Sie zur Implementierung Ihres Anwendungsfalls benötigen. Aus diesem Grund sollte die angegebene Schätzung so präzise wie möglich sein.

Note

Eine einzelne dedizierte IP-Adresse kann nur in der AWS Region verwendet werden, die Sie in diesem Schritt gewählt haben. Wenn Sie dedizierte IP-Adressen zur Verwendung in einer anderen AWS Region anfordern möchten, wählen Sie Weitere Anfrage hinzufügen, und füllen Sie dann die Region, Limit, und New limit value-Felder für die zusätzliche Region. Wiederholen Sie diesen Vorgang für jede Region, in der Sie dedizierte IP-Adressen verwenden möchten.

7. Geben Sie unter Case Description (Fallbeschreibung) als Use Case Description (Beschreibung des Anwendungsfalls) an, dass Sie dedizierte IP-Adressen anfordern möchten. Geben Sie auch an, wenn Sie eine bestimmte Anzahl von dedizierten IP-Adressen anfordern möchten. Wenn Sie keine Anzahl für die dedizierten IP-Adressen angeben, stellen wir Ihnen die Anzahl der dedizierten IP-Adressen bereit, die zum Erfüllen der im vorherigen Schritt angegebenen Senderatenanforderung erforderlich sind.

Beschreiben Sie anschließend, wie Sie die dedizierten IP-Adressen zum Senden von E-Mails mit Amazon SES verwenden möchten. Geben Sie zudem an, warum Sie dedizierte IP-Adressen anstelle von gemeinsam genutzten IP-Adressen verwenden möchten. Mit diesen Informationen können wir Ihren Anwendungsfall besser nachvollziehen.

8. Wählen Sie unter Contact options (Kontaktoptionen) als Preferred contact language (Bevorzugte Kontaktsprache) aus, ob Sie in diesem Fall auf English (Englisch) oder Japanese (Japanisch) kommunizieren möchten.
9. Wenn Sie fertig sind, klicken Sie auf Submit.

Wir bearbeiten wir Ihren Antrag, nachdem Sie das Formular übermittelt haben. Wenn wir Ihrer Anforderung entsprechen, reagieren wir im Support-Center auf Ihren Fall, um zu bestätigen, dass Ihre neuen dedizierten IP-Adressen mit Ihrem Konto verknüpft sind.

Freisetzen dedizierter IP-Adressen

Wenn Sie dedizierte IP-Adressen, die Ihrem Konto zugewiesen sind, nicht mehr benötigen, können Sie diese anhand der folgenden Schritte freigeben.

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 dedizierten IP anteilig auf Grundlage der im aktuellen Monat bereits verstrichenen Tage.

So setzen Sie dedizierte IP-Adressen frei

1. Melden Sie sich beim an.AWS Management Consoleum <https://console.aws.amazon.com/>.
2. Klicken Sie im Menü Support (Support) auf Support Center (Support-Center).
3. Wählen Sie auf der Registerkarte My support cases (Meine Support-Fälle) die Option Create case (Fall erstellen) aus.
4. Wählen Sie unter Create case (Fall erstellen) die Option Service limit increase (Erhöhung des Service Limits) aus.
5. Führen Sie unter Case classification (Fallklassifizierung) die folgenden Abschnitte aus:
 - Wählen Sie für Limit Type (Limit-Typ) die Option SES Sending Limits (SES-Sendelimits) aus.

- Geben Sie als Mail Type (E-Mail-Typ) einen beliebigen Wert an.
 - Für Meine E-Mail-Sendefunktionen entsprechen den AWS -Servicebedingungen und AUP Wählen Sie die Option aus, die Ihrem Anwendungsfall entspricht.
 - Wählen Sie unter I only send to recipients who have specifically requested my mail (Ich sende nur an Empfänger, die meine Mail explizit angefordert haben) die Option aus, die Ihrem Anwendungsfall entspricht.
 - Wählen Sie unter I have a process to handle bounces and complaints (Ich habe einen Prozess für die Verarbeitung von unzustellbaren E-Mails und Beschwerden) die Option aus, die Ihrem Anwendungsfall entspricht.
6. Führen Sie unter Requests (Anforderungen) die folgenden Abschnitte aus:
- Für Region Wählen Sie die AWS Region aus, für die Ihre Anfrage gilt.

Note

Dedizierte IP-Adressen sind für jede AWS Region eindeutig. Daher ist es wichtig, die Region auszuwählen, der die dedizierte IP-Adresse zugeordnet ist.

- Wählen Sie als Limit die Option Desired Maximum Send Rate (Gewünschte maximale Senderate) aus.
- Geben Sie als New limit value (Neuer Positionswert) eine beliebige Zahl ein. Die Anzahl, die Sie hier eingeben, ist nicht wichtig. Sie geben die Anzahl der freizugebenden dedizierten IPs im nächsten Schritt an.

Note

Eine einzelne dedizierte IP-Adresse kann nur in einer einzelnen AWS Region verwendet werden. Wenn Sie dedizierte IP-Adressen freigeben möchten, die Sie in anderen AWS Regionen verwendet haben, wählen Sie Weitere Anfrage hinzufügen. Anschließend füllen Sie für die zusätzlichen Region die Felder Region, Limit und New limit value (Neuer Limit-Wert) aus. Wiederholen Sie diesen Vorgang für jede dedizierte IP-Adresse, die Sie freigeben möchten.

7. Geben Sie unter Case Description (Fallbeschreibung) als Use Case Description (Beschreibung des Anwendungsfalls) an, dass Sie vorhandene dedizierte IP-Adressen freigeben möchten. Wenn Sie derzeit mehr als eine dedizierte IP-Adresse leasen, geben Sie die Anzahl der dedizierten IP-Adressen an, die Sie freisetzen möchten.
8. Wählen Sie unter Contact options (Kontaktoptionen) als Preferred contact language (Bevorzugte Kontaktsprache) aus, ob Sie in diesem Fall auf English (Englisch) oder Japanese (Japanisch) kommunizieren möchten.
9. Wenn Sie fertig sind, klicken Sie auf Submit.

Sobald wir Ihre Anfrage erhalten, senden wir Ihnen eine Nachricht, in der Sie dazu aufgefordert werden, die Freigabe Ihrer dedizierten IP-Adressen zu bestätigen. Nachdem Sie bestätigt haben, dass Sie die IP-Adressen freigeben möchten, werden diese aus Ihrem Konto entfernt.

Aufwärmen dedizierter IP-Adressen

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 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 IP-Adresse sollten Sie E-Mails an Ihre aktivsten Benutzer senden, um sicherzustellen, dass Ihre Beschwerdequote 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 Versandaktivitäten](#) (p. 282).

Automatisches Aufwärmen dedizierter IP-Adressen

Wenn Sie dedizierte IP-Adressen 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.

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 IP-Adressen anfordern, verteilt Amazon SES den Versand Ihrer E-Mails auf die dedizierten IP-Adressen und eine Reihe von Adressen, die mit anderen Amazon SES-Kunden geteilt werden. Amazon 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 Amazon SES den Versand Ihrer E-Mails auf die bestehenden dedizierten IPs (die bereits aufgewärmt sind) und Ihre neuen dedizierten IPs (die noch nicht aufgewärmt sind). Mit Amazon SES erhöht im Laufe der Zeit allmählich die Anzahl der Nachrichten, die über Ihre neuen dedizierten IP-Adressen versendet werden.

Note

Das automatische IP-Warm-up ist ein zeitbasierter Prozess. Der Aufwärmprozentsatz 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 Amazon SES verwenden.

Versenden Sie keine großen E-Mail-Volumen 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.

Deaktivieren des automatischen Aufwärmvorgangs

Beim Kauf neuer dedizierten IP-Adressen wärmt Amazon SES sie automatisch für Sie auf. Wenn Sie es vorziehen, dedizierte IP-Adressen selbst aufzuwärmen, können Sie die automatische Aufwärmfunktion deaktivieren.

Important

Wenn Sie die automatische Aufwärmfunktion deaktivieren, sind Sie für das Aufwärmen Ihrer dedizierten IP-Adressen selbst verantwortlich. Wenn Sie E-Mails über Adressen versenden, die noch nicht aufgewärmt sind, kann dies schlechte Zustellungsraten zur Folge haben.

So deaktivieren Sie die automatische Aufwärmfunktion

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Klicken Sie in der Navigationsleiste auf der linken Seite auf Dedicated IPs.
3. Deaktivieren Sie das Kontrollkästchen neben Automatic IP warm-up.

Neustarten des automatischen Aufwärmvorgangs

Sie können den automatischen IP-Aufwärmvorgang für einen Satz an IP-Adressen neu starten, die zu einem dedizierten IP-Pool gehören.

So starten Sie den automatischen Aufwärmvorgang neu

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Klicken Sie in der Navigationsleiste auf der linken Seite auf Dedicated IPs.
3. Wählen Sie im dedizierten IP-Pool, für den Sie den Aufwärmvorgang neu starten möchten, Actions und anschließend Restart IP warm up aus.

Der Status des automatischen Aufwärmvorgangs wird in der Spalte Warm Up Status (Aufwärmstatus) angezeigt. Wenn der Aufwärmvorgang abgeschlossen ist, wird in dieser Spalte Complete angezeigt.

Erstellen von dedizierten IP-Pools

Wenn Sie mehrere dedizierte IP-Adressen für die Verwendung mit Amazon SES erworben haben, können Sie Gruppen dieser Adressen erstellen. Diese Gruppen werden als dedizierte IP-Pools bezeichnet. Ein häufiger Anwendungsfall ist es, einen Pool von dedizierten IP-Adressen 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, die von allen Amazon SES Kunden gemeinsam genutzt werden. Der gemeinsame 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 [Verwalten von dedizierten IP-](#) (p. 278).

So erstellen Sie einen dedizierten IP-Pool mit der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich auf der linken Seite des Bildschirms unter Email Sending die Option Dedicated IPs aus.
3. Wählen Sie Create a New IP Pool aus.
4. Geben Sie auf der Seite IP Pool Name für Pool name einen beschreibenden Namen für den dedizierten IP-Pool ein und wählen Sie dann Next aus.

5. Aktivieren Sie auf der Seite Add Dedicated IPs das Kontrollkästchen neben jeder IP-Adresse, die Sie dem Pool hinzufügen möchten, und wählen Sie dann Next aus.

Note

Dedizierte IP-Adressen, die Sie noch keinem Pool zugewiesen haben, sind im ses-default-dedicated-pool enthalten. Wenn Sie eine E-Mail mit einem Konfigurationssatz senden, der keinen Sendepool angibt, oder wenn Sie eine E-Mail senden, ohne überhaupt einen Konfigurationssatz anzugeben, sendet Amazon SES die E-Mail von einer der Adressen im ses-default-dedicated-pool.

Eine dedizierte IP-Adresse kann nur zu einem einzigen Pool gehören. Wenn Sie eine dedizierte IP-Adresse auswählen, die einem anderen Pool zugeordnet ist, überschreibt Amazon SES diese Einstellung und ordnet die Adresse dem Pool zu, den Sie erstellen.

6. Führen Sie auf der Seite Assign to a configuration set eine der folgenden Aktionen aus:
 - Wählen Sie Add this pool to an existing configuration set aus, um den dedizierten IP-Pool mit einem bestehenden Konfigurationssatz zu verknüpfen. Wählen Sie dann unter Existing configuration sets (Vorhandene Konfigurationssätze) den Konfigurationssatz aus, mit dem Sie den IP-Pool verknüpfen möchten.
 - Wählen Sie Create a new configuration set aus, um einen Konfigurationssatz zu erstellen und den dedizierten IP-Pool damit zu verknüpfen. Geben Sie unter Configuration set name einen beschreibenden Namen für den Konfigurationssatz ein.

Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

7. Überprüfen Sie auf der Seite Review die Einstellungen des dedizierten IP-Pools. Wenn Sie bereit sind, den IP-Pool anzulegen, wählen Sie Create aus.

Verwenden Ihrer eigenen IP-Adressen zum Senden von E-Mails mit Amazon SES verwenden

Amazon SES enthält eine Funktion namens Eigene IP mitbringen (BYOIP). Dies ermöglicht es, Ihre eigenen IP-Adressen zum Senden von E-Mails über Amazon SES 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 über Amazon SES zur Verfügung stellen.

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 über Amazon SES versenden, ohne den Ruf Ihrer IP-Adressen wiederherstellen zu müssen.

Requirements

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.

Considerations

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 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 freigegebenen IP-Adressen verwenden müssen, können Sie Amazon SES in einer anderen AWS Region verwenden oder ein neues AWS-Konto erstellen.
- Für jede IP-Adresse, die Sie mit BYOIP verwenden, fällt eine monatliche Gebühr an. Weitere Informationen finden Sie unter [Amazon SES – Preise](#).

Verwenden Ihrer eigenen IP-Adressen mit Amazon SES

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 bitte folgende Informationen an ses-byoip-request@amazon.com:

- Ihre AWS-Konto-ID.
- Die AWS Region, in der Sie den IP-Bereich verwenden möchten, z. B. ap-south-1.
- Eine Beschreibung Ihres Anwendungsfalls
- Der IP-Bereich, den Sie mit Amazon SES verwenden 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.

Testen der E-Mail-Versendung in Amazon SES

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 \(p. 400\)](#) 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, der in Rechnung gestellte Betrag für Nachrichten, die Sie an den Postfachsimulator senden, ist derselbe wie bei denen, 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 Sendeansforderung 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 Adresse des Postfachsimulators senden, müssen Sie sie über Amazon SES senden, indem Sie die AWS CLI, ein AWS SDK, die Amazon SES S-Konsole, die Amazon SES SMTP-Schnittstelle oder die Amazon SES API. Der Postfachsimulator reagiert nicht auf E-Mails, die von externen Quellen empfangen werden.

Simuliertes Szenario	E-Mail-Adresse
Erfolgreiche Zustellung— Ihre E-Mail wird vom E-Mail-Anbieter des Empfängers angenommen. Wenn Sie Zustellungsbenachrichtigungen einrichten, wie unter Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen (p. 288) Amazon SES sendet Ihnen eine Versandbenachrichtigung über Amazon Simple Notification Service (Amazon SNS).	<code>success@simulator.amazonses.com</code>
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 Unzustellbarkeitsnachricht und sendet sie Ihnen je nach Einrichtung Ihres Kontos per E-Mail oder als Benachrichtigung an ein	<code>bounce@simulator.amazonses.com</code>

Simuliertes Szenario	E-Mail-Adresse
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 Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen (p. 288).	
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 .	<code>ooto@simulator.amazonses.com</code>
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". Je nach Kontoeinrichtung leitet Amazon SES diese Beschwerdenachricht per E-Mail an Sie weiter oder benachrichtigt ein Amazon SNS -Thema. Die vom Postfachsimulator übermittelte Beschwerdenachricht entspricht RFC 5965 . Weitere Informationen zu Rückmeldungen im Falle von Beschwerden finden Sie unter Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen (p. 288).	<code>complaint@simulator.amazonses.com</code>
Empfängeradresse in der Unterdrückungsliste— Amazon SES generiert eine feste Unzustellbarkeit, als ob die Adresse des Empfängers in der globalen Unterdrückungsliste enthalten ist.	<code>suppressionlist@simulator.amazonses.com</code>

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 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](#). Codebeispiele, die Sie verwenden können, um Nachrichten mit Anlagen zu senden, finden Sie unter [Senden von Raw-E-Mails mit AWS SDKs \(p. 478\)](#).

Verwenden der Unterdrückungsliste auf Kontoebene

Amazon SES enthält eine Unterdrückungsliste auf Kontoebene, die auf Ihr AWS Konto in der aktuellen AWS-Region zutrifft. Diese Unterdrückungsliste verhindert, dass Sie E-Mail-Nachrichten an Adressen senden, die zuvor ein Unzustellbarkeits- oder Beschwerdeereignis ausgelöst haben. Wenn Sie die Unterdrückungsliste auf Kontoebene konfigurieren, geben Sie an, ob Adressen der Liste hinzugefügt werden sollen, wenn sie zu permanenten Unzustellbarkeiten, zu Beschwerden oder zu beidem führen. Sie können einzelne oder Massenadressen manuell hinzufügen oder aus der Unterdrückungsliste auf Kontoebene entfernen, indem Sie die Amazon SES API v2 nutzen.

Note

Um Adressen im Massenformat hinzuzufügen oder zu entfernen, müssen Sie über Produktionszugriff verfügen. Weitere Informationen zur Sandbox finden Sie unter [Verlassen der Amazon SES -Sandbox \(p. 79\)](#).

Amazon SES enthält auch eine globale Unterdrückungsliste. Weitere Informationen finden Sie unter [Verwenden der globalen Unterdrückungsliste von Amazon SES \(p. 210\)](#).

Überlegungen zur Unterdrückungsliste auf Kontoebene

Sie sollten die folgenden Faktoren berücksichtigen, wenn Sie die Unterdrückungsliste auf Kontoebene verwenden:

- Wenn Sie nach dem 25. November 2019 mit der Verwendung von Amazon SES begonnen haben, wird in Ihrem Konto standardmäßig die Unterdrückungsliste auf Kontoebene sowohl für Unzustellbarkeiten als auch für Beschwerden verwendet. Wenn Sie mit der Verwendung von Amazon SES vor diesem Datum beginnen, müssen Sie diese Funktion mithilfe der `PutAccountSuppressionAttributes`-Vorgang in der Amazon SES API.
- Wenn Sie versuchen, eine Nachricht an eine Adresse in der Unterdrückungsliste auf Kontoebene zu senden, akzeptiert Amazon SES die Nachricht, sendet sie aber nicht.

- Amazon SES zählt die Nachrichten, die Sie an Adressen in der Unterdrückungsliste auf Kontoebene senden, nicht zur Unzustellbarkeitsrate für Ihr Konto.
- zählt Amazon SES die Nachrichten, die Sie an Adressen auf der Unterdrückungsliste auf Kontoebene senden, für Ihr täglich versendetes Kontingent.
- E-Mail-Adressen auf der Unterdrückungsliste auf Kontoebene bleiben dort, bis Sie sie mithilfe der [DeleteSuppressedDestinationv2](#) in der Amazon SES API.
- Wenn die Fähigkeit Ihres Kontos zum Senden von E-Mails unterbrochen wird, löscht Amazon SES automatisch nach 90 Tagen die Adressen in der Unterdrückungsliste auf Kontoebene. Wenn die Fähigkeit Ihres Kontos zum Senden von E-Mail-Nachrichten wiederhergestellt wird, bevor dieser 90-tägige Aufbewahrungszeitraum endet, werden die Adressen in der Unterdrückungsliste auf Kontoebene nicht gelöscht.
- Google Mail stellt keine Beschwerdedaten Amazon SES. 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 zur Unterdrückungsliste auf Kontoebene hinzugefügt.
- Sie können die Unterdrückungsliste auf Kontoebene aktivieren, wenn sich Ihr Konto in der Amazon SES Sandbox befindet. Sie können jedoch die [PutSuppressedDestination](#) oder [CreateImportJob](#) Vorgang bis Ihr Konto aus der Sandbox entfernt wird. Weitere Informationen zur Sandbox finden Sie unter [Verlassen der Amazon SES -Sandbox](#) (p. 79).
- Wenn Sie die Unterdrückungsliste auf Kontoebene verwenden, fügt Amazon SES der globalen Unterdrückungsliste auch Adressen hinzu, die zu permanenten Unzustellbarkeiten führen.

Aktivieren der Unterdrückungsliste auf Kontoebene

Sie können die Berechtigung [PutAccountSuppressionAttributes](#) in der Amazon SES API v2 können Sie die Unterdrückungsliste auf Kontoebene aktivieren und einrichten. 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](#).

So konfigurieren Sie mithilfe der AWS CLI die Unterdrückungsliste auf Kontoebene

- 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 die 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.

Aktivieren der Unterdrückungsliste auf Kontoebene

Sie können die Unterdrückung auf Kontoebene auch so konfigurieren, dass sie nur für bestimmte [Konfigurationssätze](#) (p. 271) 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.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So konfigurieren Sie die Unterdrückungsliste auf Kontoebene mithilfe des Befehls AWS CLI für einen Konfigurationssatz

- 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 im vorherigen Beispiel **configSet** durch den Namen des Konfigurationssatzes, der die Unterdrückungsliste auf Kontoebene verwenden soll.

Manuelles Hinzufügen von einzelnen E-Mail-Adressen zur Unterdrückungsliste auf Kontoebene

Sie können einzelne Adressen manuell zur Unterdrückungsliste auf Kontoebene hinzufügen, indem Sie die [PutSuppressedDestinationv2](#) in der Amazon SES API. Es gibt keine Begrenzung für die Anzahl der Adressen, die Sie der Unterdrückungsliste auf Kontoebene hinzufügen können.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So fügen Sie mithilfe der AWS CLI manuell eine Adresse zur Unterdrückungsliste auf Kontoebene hinzu

- 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
```

Ersetzen Sie im vorherigen Beispiel **recipient@example.com** durch die E-Mail-Adresse, die Sie der Unterdrückungsliste auf Kontoebene hinzufügen möchten, und **BOUNCE** durch den Grund, aus dem Sie die Adresse zur Unterdrückungsliste hinzufügen (zulässige Werte sind **BOUNCE** und **COMPLAINT**).

Massenanordnung von E-Mail-Adressen zur Unterdrückungsliste auf Kontoebene

Sie können Adressen manuell in Massenmengen hinzufügen, indem Sie zuerst Ihre Kontaktliste in ein Amazon S3 Objekt hochladen, auf das Sie zugreifen können, gefolgt von der [CreateImportJobv2](#) in der Amazon SES API.

Note

Es gibt keine Begrenzung für die Anzahl der Adressen, die Sie der Unterdrückungsliste auf Kontoebene hinzufügen können. Es gibt jedoch eine Begrenzung für die Massenanfügung von 1.000.000 Adressen in einem Amazon S3 Objekt pro API-Aufruf.

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 Zeilenumbrüche getrennte JSON-Dateien werden unterstützt. In diesem Format ist jede Zeile ein vollständiges JSON-Objekt mit einer einzelnen Adressdefinition.

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 obigen Beispielen den Befehl **recipient1@example.com** und **recipient2@example.com** mit den E-Mail-Adressen, die Sie der Unterdrückungsliste auf Kontoebene hinzufügen möchten. Die zulässigen Gründe, aus denen Sie die Adressen zur Unterdrückungsliste hinzufügen, sind **BOUNCE** und **COMPLAINT**.

- Verwenden der [CreateImportJobv2](#) in der Amazon SES API.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So fügen Sie mithilfe der manuell Massendressen zur Unterdrückungsliste auf Kontoebene hinzu AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

Linux, macOS, or Unix

```
aws sesv2 create-import-job \  
--import-destination "{\"SuppressionListDestination\":  
  {\"SuppressionListImportAction\": \"PUT\"}}\" \  
--import-data-source "{\"S3Url\": \"s3://s3bucket/s3object\", \"DataFormat\": \"CSV  
\"}"
```

Windows

```
aws sesv2 create-import-job ^  
--import-destination "{\"SuppressionListDestination\":  
  {\"SuppressionListImportAction\": \"PUT\"}}\" ^  
--import-data-source "{\"S3Url\": \"s3://s3bucket/s3object\", \"DataFormat\": \"CSV  
\"}"
```

Ersetzen Sie in den obigen Beispielen den Befehl *S3 Bucket* und *s3object* mit dem Amazon S3 Bucket-Namen und dem Amazon S3-Objektnamen.

Anzeigen einer Liste der Adressen, die sich in der Unterdrückungsliste auf Kontoebene befinden

Sie können eine Liste aller E-Mail-Adressen anzeigen, die sich in Ihrem Konto in der Unterdrückungsliste auf Kontoebene befinden, indem Sie die [ListSuppressedDestinationsv2](#) in der Amazon SES API.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

Anzeigen einer Liste aller E-Mail-Adressen, die sich in der 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 der Unterdrückungsliste auf Kontoebene befinden. Die Ausgabe sieht in etwa folgendermaßen aus:

```
{  
  "SuppressedDestinationSummaries": [  
    {  
      "EmailAddress": "recipient2@example.com",  
      "Reason": "COMPLAINT",  
      "LastUpdateTime": 1586552585.077  
    },  
    {  
      "EmailAddress": "recipient0@example.com",  
      "Reason": "COMPLAINT",  
      "LastUpdateTime": 1586552666.613  
    },  
  ],  
}
```

```
{
  "EmailAddress": "recipient1@example.com",
  "Reason": "BOUNCE",
  "LastUpdateTime": 1586556479.141
}
```

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 der 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 der 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.

Sie können in der Linux-, macOS - oder Unix-Befehlszeile auch die integrierte `grep`, um nach bestimmten Adressen oder Domänen zu suchen.

Suchen einer bestimmten Adresse in der 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 gesucht werden soll.

Entfernen einer E-Mail-Adresse aus der Unterdrückungsliste auf Kontoebene

Wenn eine Adresse zur Unterdrückungsliste für Ihr Konto hinzugefügt wird, Sie aber wissen, dass die Adresse nicht auf die Liste gehört, können Sie sie manuell mithilfe von [DeleteSuppressedDestinationv2](#) in der Amazon SES API.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So entfernen Sie mithilfe der AWS CLI eine Adresse aus der Unterdrückungsliste auf Kontoebene

- 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 im vorherigen Beispiel *recipient@example.com* durch die E-Mail-Adresse, die Sie von der Unterdrückungsliste auf Kontoebene entfernen möchten.

Entfernen einer Massenanordnung von E-Mails aus der Unterdrückungsliste auf Kontoebene

Sie können Adressen manuell entfernen, indem Sie zuerst Ihre Kontaktliste in ein Amazon S3 Objekt hochladen, auf das Sie zugreifen können, gefolgt von der [CreateImportJobv2](#) in der Amazon SES API.

Note

Es gibt keine Begrenzung für die Anzahl der Adressen, die Sie aus der Unterdrückungsliste auf Kontoebene entfernen können. Es gibt jedoch eine Begrenzung für die Massennöschung von 10.000 Adressen in einem Amazon S3 Objekt pro API-Aufruf.

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 Zeilenumbrüche getrennte JSON-Dateien werden unterstützt. In diesem Format ist jede Zeile ein vollständiges JSON-Objekt mit einer einzelnen Adressdefinition.

Beispiel für das JSON-Format zum Hinzufügen von Adressen:

```
{"emailAddress": "recipient3@example.com"}
```

Ersetzen Sie in den obigen Beispielen den Befehl *recipient3@example.com* mit den E-Mail-Adressen, die Sie von der Unterdrückungsliste auf Kontoebene entfernen möchten.

- Verwenden der [CreateImportJobv2](#) in der Amazon SES API.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So entfernen Sie mithilfe der manuell Massendressen aus der Unterdrückungsliste auf KontoebeneAWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

Linux, macOS, or Unix

```
aws sesv2 create-import-job \
--import-destination "{\"SuppressionListDestination\":
  {\"SuppressionListImportAction\": \"DELETE\"}}\" \
--import-data-source "{\"S3Url\": \"s3://s3bucket/s3object\", \"DataFormat\": \"CSV
\"}\""
```

Windows

```
aws sesv2 create-import-job ^
--import-destination "{\"SuppressionListDestination\":
  {\"SuppressionListImportAction\": \"DELETE\"}}\" ^
--import-data-source "{\"S3Url\": \"s3://s3bucket/s3object\", \"DataFormat\": \"CSV
\"}\""
```

Ersetzen Sie in den obigen Beispielen den Befehl **S3 Bucket** und **s3objekt** mit dem Amazon S3 Bucket-Namen und dem Amazon S3-Objektnamen.

Anzeigen einer Liste der Importaufträge für das Konto

Sie können eine Liste aller E-Mail-Adressen anzeigen, die sich in Ihrem Konto in der Unterdrückungsliste auf Kontoebene befinden, indem Sie die [ListImportJobsv2](#) in der Amazon SES API.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So zeigen Sie eine Liste aller Importaufträge für das Konto an

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 list-import-jobs
```

Mit dem obigen Befehl werden alle Importaufträge für das Konto zurückgegeben. Die Ausgabe sieht in etwa folgendermaßen aus:

```
{
  "ImportJobs": [
    {
      "CreatedTimestamp": 1596175615.804,
      "ImportDestination": {
```



```
        "SuppressionListDestination": {
          "SuppressionListImportAction": "PUT"
        }
      },
      "JobStatus": "COMPLETED",
      "JobId": "755380d7-fbdb-4ed2-a9a3-06866220f5b5"
    },
    {
      "CreatedTimestamp": 1596134732.398,
      "ImportDestination": {
        "SuppressionListDestination": {
          "SuppressionListImportAction": "DELETE"
        }
      },
      "JobStatus": "COMPLETED",
      "JobId": "076683bd-a7ee-4a40-9754-4ad1161ba8b6"
    },
    {
      "CreatedTimestamp": 1596645918.134,
      "ImportDestination": {
        "SuppressionListDestination": {
          "SuppressionListImportAction": "PUT"
        }
      },
      "JobStatus": "COMPLETED",
      "JobId": "6e261869-bd30-4b33-b1f2-9e035a83a395"
    }
  ]
}
```

Abrufen von Informationen über einen Importauftrag für das Konto

Sie können Informationen zu einem Importauftrag für das Konto abrufen, indem Sie die [GetImportJobv2](#) in der Amazon SES API.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So rufen Sie Informationen zu einem Importauftrag für das Konto ab

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 get-import-job --job-id JobId
```

Im obigen 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": 1597251915.243,
  "FailedRecordsCount": 1,
  "ImportDestination": {
    "SuppressionListDestination": {
      "SuppressionListImportAction": "PUT"
    }
  },
  "CompletedTimestamp": 1597252002.583
}
```

Deaktivieren der Unterdrückungsliste auf Kontoebene

Sie können die Berechtigung `PutAccountSuppressionAttributes`-Vorgang in der Amazon SES -API v2 verwenden, um die Unterdrückungsliste auf Kontoebene effektiv zu deaktivieren, indem Sie die Werte aus dem `demsuppressed-reasons`-Attribut.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So deaktivieren Sie mithilfe der AWS CLI die Unterdrückungsliste auf Kontoebene

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 put-account-suppression-attributes --suppressed-reasons
```

Verwenden der globalen Unterdrückungsliste von Amazon SES

Amazon SES enthält eine globale Unterdrückungsliste. Wenn ein Amazon SES Kunde eine E-Mail sendet, die zu einer permanenten Unzustellbarkeit führt, fügt Amazon SES die E-Mail-Adresse, die die Unzustellbarkeit erzeugt hat, zu einer globalen Unterdrückungsliste hinzu. Die globale Unterdrückungsliste lautet global in dem Sinne, dass dies für alle Amazon 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 Amazon SES die Nachricht, sendet sie aber nicht, da die E-Mail-Adresse unterdrückt wird. Ein Vorteil der globalen Unterdrückungsliste besteht darin, dass sie standardmäßig für alle Amazon SES Konten gilt. Sie müssen keine zusätzliche Konfiguration durchführen, um sie zu verwenden. Ein Nachteil ist, dass Sie die globale Unterdrückungsliste nicht abfragen können, da sie E-Mail-Adressen enthält, die den Konten anderer Amazon SES -Benutzer von zugeordnet sind. Außerdem können Sie der globalen Unterdrückungsliste keine Adressen manuell hinzufügen, und Sie können Adressen nur mithilfe der Amazon SES Konsole aus der globalen Unterdrückungsliste entfernen.

Amazon SES enthält auch eine Unterdrückungsliste auf Kontoebene. Weitere Informationen finden Sie unter [Verwenden der Unterdrückungsliste auf Kontoebene \(p. 201\)](#).

Überlegungen zur globalen Unterdrückungsliste

Sie sollten die folgenden Faktoren berücksichtigen, wenn Sie die globale Unterdrückungsliste verwenden:

- Die globale Unterdrückungsliste ist standardmäßig für alle Amazon SES Konten aktiviert. Sie können es nicht deaktivieren.
- Da Amazon 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 Amazon SES die Adresse der globalen Unterdrückungsliste für einen kurzen Zeitraum hinzu. Nach Ablauf dieses Zeitraums entfernt Amazon SES die Adresse aus der Liste. Wenn die Adresse einen weiteren Hard Bounce erzeugt, fügt Amazon 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 Adresse kann bis zu 14 Tagen in der globalen Unterdrückungsliste verbleiben.
- Wenn Sie versuchen, eine Nachricht an eine Adresse in der globalen Unterdrückungsliste zu senden, akzeptiert Amazon SES die Nachricht, sendet sie aber nicht. Amazon SES generiert eine Bounce-Benachrichtigung mit einem `bounceTypeWert` von `Permanent`, und ein `bounceSubTypeWert` 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.
- zählt Amazon SES die Nachrichten, die Sie an Adressen in der globalen Unterdrückungsliste senden, zur Unzustellbarkeitsrate für Ihr Konto.
- zählt Amazon SES die Nachrichten, die Sie an Adressen in der globalen Unterdrückungsliste senden, für Ihr täglich versendetes Kontingent.
- 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 Unzustellbarkeitsquote zu hoch wird, legen wir möglicherweise eine Prüfung für Ihr Konto fest oder unterbrechen die Fähigkeit Ihres Kontos zum Versenden von E-Mails.

Entfernen einer Adresse aus der globalen Unterdrückungsliste

Wenn Sie sicher sind, dass eine Adresse auf der globalen Unterdrückungsliste eigentlich gültig ist, können Sie sie mithilfe der folgenden Vorgehensweise entfernen. Wenn Sie eine Adresse aus der globalen Unterdrückungsliste in einer Region entfernen, gilt die Entfernung für alle AWS Konten in allen Regionen.

So entfernen Sie eine E-Mail-Adresse aus der globalen Unterdrückungsliste

1. Melden Sie sich beim `an.AWS Management Console` und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie mit der Auswahl „Region“ in der oberen rechten Ecke des Fensters eine der folgenden AWS Regionen aus: USA Ost (Nord-Virginia), USA West (Oregon) oder Europa (Irland). Die bestimmte ausgewählte Region ist nicht wichtig, da die Unterdrückungsliste für alle Regionen gleichermaßen gilt.

Note

Um dieses Verfahren abzuschließen, müssen Sie eine der im vorstehenden Absatz aufgeführten AWS Regionen verwenden. Sie können dieses Verfahren in anderen AWS Regionen nicht abschließen.

3. Wählen Sie im Navigationsbereich Unterdrückungslisten-Entfernung aus.
4. Geben Sie im Feld Email Address (E-Mail-Adresse) die E-Mail-Adresse ein, die Sie aus der globalen Unterdrückungsliste entfernen möchten.
5. Geben Sie im Feld Type characters die darüber abgebildeten Zeichen ein.
6. Klicken Sie auf Submit (Absenden).

Wenn sich die von Ihnen angegebene E-Mail-Adresse in der globalen Unterdrückungsliste befindet, entfernen wir sie sofort.

Verwenden von Listenverwaltung

Amazon SES bietet Funktionen zur Listenverwaltung, d. h. Kunden können ihre eigenen Mailinglisten, die als Kontaktlisten bezeichnet werden, verwalten. A **Kontaktliste** ist eine Liste, mit der Sie alle Ihre Kontakte speichern können, die ein bestimmtes Thema oder bestimmte Themen abonniert haben. A **contactist** ein Endbenutzer, der Ihre E-Mails erhält. A **Thema** ist eine Interessengruppe, ein Design oder ein Label innerhalb einer Liste. Listen können mehrere Themen haben.

Verwenden der [ListKontakte](#) in der Amazon SES API v2 verwenden, können Sie eine Liste aller Kontakte abrufen, die ein bestimmtes Thema abonniert haben, an die Sie E-Mails mit dem [SendEmail](#) verwenden.

Sie können einzelne oder Massenadressen manuell hinzufügen oder aus der Unterdrückungsliste auf Kontoebene entfernen, indem Sie die Amazon SES API v2 nutzen.

Note

Um Adressen im Massenformat hinzuzufügen oder zu entfernen, müssen Sie über Produktionszugriff verfügen. Weitere Informationen zur Sandbox finden Sie unter [Verlassen der Amazon SES -Sandbox](#) (p. 79).

Informationen zur Abonnementverwaltung finden Sie unter [Verwenden der Abonnementverwaltung](#) (p. 218).

Übersicht über die Listenverwaltung

Sie sollten die folgenden Faktoren berücksichtigen, wenn Sie die Listenverwaltung verwenden:

- Sie können Listenthemen beim Erstellen der Liste angeben.
- Pro AWS Konto ist nur eine Kontaktliste zulässig.
- Eine Liste kann maximal 20 Themen umfassen.
- Sie können eine vorhandene Kontaktliste aktualisieren, einschließlich dem Hinzufügen neuer Themen zur Liste, dem Hinzufügen oder Löschen von Kontakten aus einer Liste und dem 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 in Amazon SES importieren, indem Sie die [CreateImportJob](#)-API.
- Amazon SES sendet eine E-Mail zurück, wenn sie an einen nicht abonnierten Kontakt in Ihrer Kontaktliste gesendet wird. Weitere Informationen finden Sie unter [Verwenden der Abonnementverwaltung](#) (p. 218) .
- Jedem Kontakt kann zugeordnete Attribute aufweisen, mit denen Sie Informationen zu diesem Kontakt speichern können.

Konfigurieren der Listenverwaltung

Sie können die folgenden -Operationen verwenden, um Listenverwaltungsfunktionen zu konfigurieren. Eine vollständige Liste der Kontaktlisten und der Kontaktoperationen finden Sie im [Amazon SES API v2-Referenz](#).

Erstellen einer Kontaktliste

Sie können die Berechtigung [CreateContactList](#) in der Amazon 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 zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So erstellen Sie eine Kontaktliste mithilfe der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 create-contact-list --cli-input-json file://CONTACT-LIST-JSON
```

Ersetzen Sie im Befehl oben den Befehl oben **KONTAKT-LIST-JSON** mit dem Pfad zu Ihrer JSON-Datei für Ihre [CreateContactList](#)-Anfrage.

Ein Beispiel für CreateContactList-Eingabe-JSON-Datei für die Anforderung lautet 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"
    }
  ]
}
```

Erstellen eines Kontakts

Sie können die Berechtigung [CreateContact](#)-Vorgang in der Amazon 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 zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

So erstellen Sie einen Kontakt mit der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 create-contact --cli-input-json file://CONTACT-JSON
```

Ersetzen Sie im Befehl oben den Befehl oben **CONTACT-JSON** mit dem Pfad zu Ihrer JSON-Datei für Ihre [CreateContact](#) request.

Ein Beispiel für CreateContact Eingabe-JSON-Datei für die Anforderung lautet wie folgt:

```
{
  "ContactListName": "ExampleContactListName",
  "EmailAddress": "example@amazon.com",
  "UnsubscribeAll": false,
  "TopicPreferences": [
    {
      "TopicName": "Sports",
      "SubscriptionStatus": "OPT_IN"
    }
  ],
  "AttributesData": "{\"Name\": \"John\", \"Location\": \"Seattle\"}"
}
```

Im obigen Beispiel wird der unsubscribeAll-Wert von `false` gezeigt an, dass sich der Kontakt nicht von allen Themen abgemeldet hat, wobei der Wert `true` würde bedeuten, 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“.

Die AttributeData 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 als Massenspeicher hinzufügen, indem Sie zuerst Ihre Kontakte in ein Amazon S3 Objekt hochladen, auf das Sie zugreifen können, gefolgt von der [CreateImportJobv2](#) in der Amazon SES API.

Sie sollten eine Kontaktliste erstellen, bevor Sie Ihre Kontakte importieren.

Note

Sie können einer Kontaktliste pro ImportJob bis zu 1 Million Kontakte 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 obigen Beispielen den Befehl `example1@amazon.com` und `example2@amazon.com` mit den E-Mail-Adressen, die Sie der Kontaktliste hinzufügen möchten. Ersetzen Sie die AttributeData-Werte durch die für den Kontakt spezifischen Werte. Ersetzen Sie außerdem *Sport* und *Radfahren* mit dem TopicName, der für Ihren Kontakt gilt. Die akzeptablen 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	Beschreibung
emailAddress	Die E-Mail-Adresse des Kontakts. Dies ist ein obligatorisches Feld.

Attribut	Beschreibung
<code>unsubscribeAll</code>	Ein boolescher Wertstatus, der angibt, ob der Kontakt von allen Themen der Kontaktliste abgemeldet wird.
<code>topicPreferences</code>	Die Präferenzen des Kontakts für die Opt-In oder Opt-Out von Themen.
<code>attributesData</code>	Die Attributdaten, die einem Kontakt zugeordnet sind.

- Verwenden der [CreateImportJobv2](#) in der Amazon SES API.

Note

Im folgenden Verfahren wird davon ausgegangen, dass Sie den AWS CLI bereits installiert haben. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

Zum manuellen Hinzufügen von Kontakten in Massenmedien zu Ihrer Kontaktliste mithilfe des AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

Linux, macOS, or Unix

```
aws sesv2 create-import-job \
--import-destination "{\"ContactListDestination\": {\"ContactListName\":
\\\"ExampleContactListName\\\", \"ContactListImportAction\": \"PUT\"}}\" \
--import-data-source "{\"S3Url\": \"s3://s3bucket/s3object\", \"DataFormat\": \"CSV
\\\"}\""
```

Windows

```
aws sesv2 create-import-job ^
--import-destination "{\"ContactListDestination\": {\"ContactListName\":
\\\"ExampleContactListName\\\", \"ContactListImportAction\": \"PUT\"}}\" ^
--import-data-source "{\"S3Url\": \"s3://s3bucket/s3object\", \"DataFormat\": \"CSV
\\\"}\""
```

Ersetzen Sie in den obigen Beispielen den Befehl **S3 Bucket** und **s3objekt** mit dem Amazon S3 Bucket-Namen und dem Amazon S3-Objektnamen.

Listen Sie Ihre Kontakte auf, um ihnen E-Mails zu senden

Sie können die Berechtigung [ListKontakte](#) verwenden, um eine Liste aller Kontakte abzurufen, die ein bestimmtes Thema abonniert haben, in Verbindung mit dem [SendEmail](#)-Operation, mit der Sie ihnen E-Mails senden können.

Zum Auflisten von Kontakten mithilfe der AWS CLI

1. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws sesv2 list-contacts --cli-input-json file://LIST-CONTACTS-JSON
```


Ersetzen Sie im Befehl oben den Befehl oben **LIST-CONTACTS-JSON** mit dem Pfad zu Ihrer JSON-Datei für Ihre **ListKontakte**request.

Ein Beispiel für ListContacts Eingabe-JSON-Datei für die Anforderung ist wie folgt:

```
{
  "ContactListName": "ExampleContactListName",
  "Filter": {
    "FilteredStatus": "OPT_IN",
    "TopicFilter": {
      "TopicName": "Cycling",
      "UseDefaultIfPreferenceUnavailable": true
    }
  },
  "PageSize": 50
}
```

Der FilteredStatus zeigt den Abonnementstatus an, für den Sie filtern möchten, der entweder **OPT_IN** oder **OPT_OUT**.

Der TopicFilter ist ein optionaler Filter, der angibt, für welches Thema Sie Ergebnisse wünschen, und im obigen Beispiel ist „Cycling“.

UseDefaultIfPreferenceUnavailable kann den Wert **true** oder **false**. 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. Nachdem Sie die Kontakte in Ihrer Liste mit den oben genannten **ListKontakte** verwenden Sie den **SendEmail** Vorgang, um E-Mails an jeden Ihrer Kontakte zu senden. Bei Verwendung der Berechtigung „**SendEmail**“ können Sie **ListManagementOptions** angeben, damit Amazon SES Abmeldelinks zu Ihrer E-Mail hinzufügen kann. Weitere Informationen finden Sie unter [Verwenden der Abonnementverwaltung \(p. 218\)](#).

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.

Amazon SES sendet eine E-Mail zurück, wenn sie an einen nicht abonnierten Kontakt in Ihrer Kontaktliste gesendet wird. Dies bedeutet, dass Sie Ihre **SendEmail** -Anfragen nicht aktualisieren müssen, um das Senden an Kontakte zu vermeiden, die sich abgemeldet haben.

Um den **SendEmail** -Vorgang zu verwenden, geben Sie den **ContactListName** und **TopicName** ein, zu dem die E-Mail gehört. Der **TopicName** ist optional.

```
ListManagementOptions:
  String contactListName
  String topicName
```

3. Sie können aber auch die verwenden **X-SES-LIST-MANAGEMENT-OPTIONS**-Header, um beim Senden von E-Mails über die SMTP-Schnittstelle eine Liste und einen Topic-Namen 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}
```

Verwenden der Abonnementverwaltung

Amazon SES bietet eine Abonnementverwaltungsfunktion, bei der Amazon SES automatisch die Abmeldelinks in jeder ausgehenden E-Mail aktiviert, wenn Sie die Kontaktlistenname und TopicName in ListManagementOptions im Feld [SendEmail](#)-Vorgangsanforderung.

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 Abonnementverwaltung ist für diejenigen verfügbar, die [Einfache DKIM in Amazon SES \(p. 143\)](#), 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.

Informationen zur Listenverwaltung finden Sie unter [Verwenden von Listenverwaltung \(p. 212\)](#).

Übersicht über die Abonnementverwaltung

Sie sollten die folgenden Faktoren berücksichtigen, wenn Sie die 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 \(p. 271\)](#).
- Sie müssen die Kontaktliste angeben, während Sie die E-Mail senden. Die Abonnementverwaltung über die Link-Unsubscribe Kopf- und Fußzeilenlinks wird entsprechend behandelt.
- Amazon SES fügt Unterstützung für die Header-Standards „List-Abmelden“ hinzu, die es E-Mail-Clients und Posteingangsanbietern ermöglichen, einen Abmelde-Link oben in der E-Mail anzuzeigen, wenn sie diese unterstützen.
- List-Abmeldekopfzeilen folgen folgendem Verhalten:

Wenn ein Kontakt in einer E-Mail auf den Kopfzeilenlink List-Abbestellen 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, d. `h.OPT_IN` oder `h.OPT_OUT`, für alle Themen in einer bestimmten Liste. Die Zielseite bietet auch die Möglichkeit, sich von allen Themen in der Liste abzumelden.
- Sie müssen einen Platzhalter in Ihre E-Mails einfügen, um anzugeben, wo Amazon SES die Abmelde-URL einfügen muss. Sie können den Platzhalter maximal zwei Mal einschließen. Wenn mehr als zwei Mal verwendet werden, werden nur die ersten beiden Vorkommen ersetzt.
- Der Link „List-Abmelden“ -Kopf- und Fußzeile werden nur hinzugefügt, wenn die E-Mail an einen einzelnen Empfänger gesendet wird und der Platzhalter vorhanden sein muss, um den Abmelde-Link hinzuzufügen.
- Bei Transaktions-E-Mails, bei denen Sie nicht möchten, dass Kontakte sich abmelden können, können Sie das Feld ListManagementOptions mit Ihrem [SendEmail](#)request.

Hinzufügen eines Link zum Abmelden der Fußzeile

Verwenden Sie das `{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-Inhaltstypen unterstützt.

Sie können den Platzhalter maximal zwei Mal einschließen. Wenn mehr als zwei Mal verwendet werden, werden nur die ersten beiden Vorkommen ersetzt.

Überlegungen zur Abmeldung

Die Abonnementverwaltung über einen Abmeldekopf wird durch die folgenden beiden Kopfzeilen aktiviert, die Amazon SES hinzufügt. Wenn Sie diese Kopfzeilen in Ihrer eigenen E-Mail hinzufügen, bevor Sie sie an Amazon SES senden, überschreibt Amazon SES sie, wenn Sie ListManagementOptions aktiviert haben.

List-Unsubscribe

List-Unsubscribe-Post

Kontakte, die sich abmelden, indem sie auf den Link klicken, der in der Abmeldekopfzeile bereitgestellt wird, haben je nach E-Mail-Client oder Posteingangsanbieter eine andere Erfahrung. Benutzer, die sich über den Link in der Kopfzeile abmelden, können nicht auswählen, von welchen Themen sie sich abmelden, und sie werden von dem Thema abgemeldet, an das die E-Mail gesendet wurde.

Weitere Informationen zu Nachrichtenkopfzeilen finden Sie unter [RFC 2369](#) und [RFC 8058](#).

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 Receiver übermittelt.

E-Mail-Absender an Amazon SES

Welches Sicherheitsprotokoll Sie verwenden, um eine Verbindung mit Amazon SES 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 S-API (entweder direkt oder über ein AWS SDK) verwenden, wird die gesamte Kommunikation mit TLS über den HTTPS-Endpunkt von Amazon SES verschlüsselt. Der HTTPS-Endpunkt von Amazon SES unterstützt TLS 1.2, TLS 1.1 und TLS 1.0.

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.

- STARTTLSSTARTTLS 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, TLS 1.1, TLS 1.0 und SSLv2Hello.
- 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, TLS 1.1 und TLS 1.0.

Weitere Informationen zum Herstellen einer Verbindung mit der SMTP-Schnittstelle von Amazon SES mithilfe dieser Methoden finden Sie unter [Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt](#) (p. 100).

Amazon SES an Empfänger

Für TLS-Verbindungen unterstützt Amazon SES TLS 1.2, TLS 1.1 und TLS 1.0.

Standardmäßig verwendet Amazon SES opportunistische TLS. Das bedeutet, dass Amazon SES immer versucht, eine sichere Verbindung mit dem empfangenden Mail-Server herzustellen. Wenn Amazon SES keine sichere Verbindung herstellen kann, wird die Nachricht unverschlüsselt gesendet.

Sie können dieses Verhalten ändern, indem Sie Konfigurationssätze verwenden. Stellen Sie mithilfe der API-Operation [PutConfigurationSetDeliveryOptions](#) die Eigenschaft `TlsPolicy` für einen Konfigurationssatz auf `Require` ein. 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 ses put-configuration-set-delivery-options --configuration-set-name MyConfigurationSet --delivery-options TlsPolicy=Require
```

Im vorherigen Beispiel ersetzen Sie **MyConfigurationSet** durch den Namen des Konfigurationssatzes.

Wenn Sie unter Verwendung dieses Konfigurationssatzes eine E-Mail senden, sendet Amazon SES 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 mit Amazon SES Nachrichten senden, die mit S/MIME oder PGP verschlüsselt wurden. Nachrichten, die diese Protokolle verwenden, werden vom Sender verschlüsselt. Ihre Inhalte können nur von Empfängern angezeigt werden, die die öffentlichen Schlüssel besitzen, die zum Entschlüsseln der Nachrichten erforderlich sind.

Amazon SES unterstützt die folgenden MIME-Typen, mit denen Sie S/MIME-verschlüsselte E-Mails senden 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`

Empfangen von E-Mails mit Amazon SES

Amazon Simple Email Service (Amazon SES) ist ein E-Mail-Server, der in Ihrem Namen sowohl E-Mails senden als auch empfangen kann. Wenn Sie Amazon SES für den Empfang Ihrer E-Mails verwenden, verarbeitet Amazon SES zugrunde liegende Operationen zum Empfang von E-Mails, wie z. B.:

- Kommunizieren mit anderen E-Mail-Servern
- Prüfen auf Spam und Viren
- Ablehnen von E-Mails aus nicht vertrauenswürdigen Quellen
- Akzeptieren von E-Mails für Empfänger in Ihrer Domäne

Wenn Sie E-Mails empfangen, verarbeitet Amazon SES sie Ihren Anweisungen entsprechend. Amazon SES kann beispielsweise eingehende E-Mails einem Amazon S3 Bucket zustellen, sie in einem Amazon SNS -Thema veröffentlichen oder an Amazon WorkMail senden. Sie können auch Regeln erstellen, die explizit alle Nachrichten von bestimmten IP-Adressbereichen blockieren oder zulassen oder die automatisch Unzustellbarkeitsnachrichten senden, wenn Nachrichten an bestimmte E-Mail-Adressen gesendet werden.

Note

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 sich E-Mails über einen E-Mail-Client senden und empfangen lassen, können Sie verwenden [Amazon WorkMail](#) aus.

Amazon SES unterstützt 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 für Amazon Simple Email Service](#) in der Allgemeinen AWS Referenz.

Themen in diesem Abschnitt:

- [Konzepte Amazon SES den E-Mail-Empfang](#) (p. 222)
- [Erste Schritte zum Empfangen von E-Mails mit Amazon SES](#) (p. 224)
- [Einrichten von Amazon SES E-Mail-Empfang](#) (p. 230)
- [Amazon SES E-Mail-Empfang in Amazon SES verwalten](#) (p. 252)

Konzepte Amazon SES 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, die eine differenzierte Kontrolle über Ihre E-Mails ermöglicht, besteht darin, die auszuführenden Aktionen auf der Grundlage des Empfängers anzugeben. Die andere Methode ist, E-Mails basierend auf der ursprünglichen IP-Adresse zu blockieren oder zuzulassen. In diesem Thema werden beide Methoden beschrieben.

Kontrolle auf der Grundlage des Empfängers

Die primäre Möglichkeit zur Kontrolle Ihrer eingehenden E-Mails besteht darin, festzulegen, wie E-Mails basierend auf dem jeweiligen Empfänger behandelt werden sollen. 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. Die Liste der von Ihnen angegebenen Empfänger wird als Bedingung bezeichnet.

Sie richten Empfangsregeln ein, um festzulegen, wie mit den E-Mails zu verfahren ist, wenn eine Bedingung erfüllt ist. Eine Empfangsregel besteht aus einer Bedingung und einer sortierten Liste mit Aktionen. Wenn der Empfänger, an den die eingehende E-Mail adressiert ist, mit einem Empfänger übereinstimmt, der in der Bedingung enthalten ist, dann führt Amazon SES die Aktionen aus, die in der Regel festgelegt sind. Verfügbar sind die nachfolgend aufgeführten Aktionen:

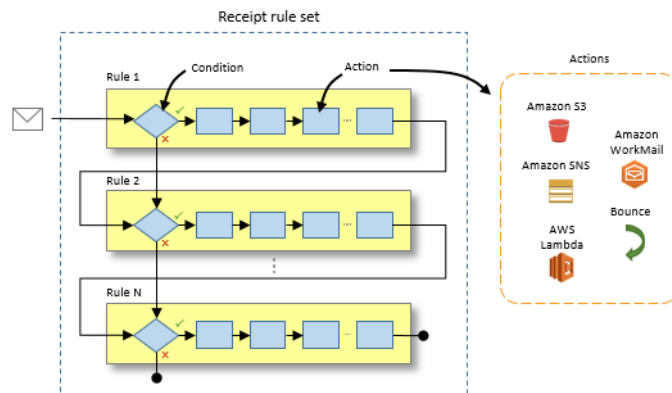
- **S3-Aktion**Stellt die E-Mail einem Amazon S3 Bucket zu und benachrichtigt Sie optional über Amazon SNS.
- **SNS-Aktion**Veröffentlicht die E-Mail in einem Amazon SNS -Thema.

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.

- **Lambda Aktion**Ruft Ihren Code über eine Lambda Funktion auf und benachrichtigt Sie optional über Amazon SNS.
- **„Bounce“-Aktion**Lehnt die E-Mail mit einer Unzustellbarkeitsnachricht an den Sender ab und benachrichtigt Sie optional über Amazon SNS.
- **Stop-Aktion**Beendet die Auswertung des Empfangsregelsatzes und benachrichtigt Sie optional über Amazon SNS.
- **Add header**Fügt der empfangenen E-Mail einen Header hinzu. Diese Aktion wird normalerweise nur in Kombination mit anderen Aktionen verwendet.
- **WorkMail Aktion**Bearbeitet die E-Mail mit Amazon WorkMail. Diese Aktion verwenden Sie in der Regel nicht direkt, da Amazon WorkMail kümmert die Einrichtung vornimmt.

Empfangsregeln werden in Empfangsregelsätze gruppiert. Sie können mehrere Empfangsregelsätze für Ihr AWS Konto definieren, aber es kann jeweils nur ein Empfangsregelsatz aktiv sein. Die folgende Abbildung zeigt, wie Empfangsregeln, Empfangsregelsätze und Aktionen miteinander in Beziehung stehen.



IP-adressbasierte Steuerung

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 abgelehnt 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 der IP-Adressen, die für das Senden von Spam bekannt sind. Sie können jedoch angeben, ob E-Mails von diesen IP-Adressen empfangen werden sollen, indem Sie sie in Ihre Zulassungsliste aufnehmen.

Note

Wenn Sie möchten, dass E-Mails, die von einer Amazon EC2 IP-Adresse stammen, zugelassen werden, müssen Sie sie der Zulassungsliste hinzufügen. Alle E-Mails, die von Amazon EC2 stammen, sind standardmäßig blockiert.

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 Zulassungsliste 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.
3. Wenn es keine Übereinstimmungen gibt, lehnt Amazon SES die E-Mail ab. Andernfalls akzeptiert Amazon SES die E-Mail.
4. Wenn Amazon SES die E-Mail akzeptiert, wertet es Ihren aktiven Empfangsregelsatz aus. Alle Empfangsregeln, die mindestens einer der Empfängerbedingungen entsprechen, werden in der Reihenfolge angewendet, in der sie definiert wurden, es sei denn, eine Aktion oder eine Empfangsregel beendet die Auswertung des Empfangsregelsatzes explizit.

Nachdem Sie sich den Prozess in der Übersicht angesehen haben, können Sie die ersten Schritte unter [Einrichten des E-Mail-Empfangs](#) in (p. 230) ausführen.

Erste Schritte zum Empfangen von E-Mails mit Amazon SES

In diesem Tutorial erstellen Sie ein AWS Konto, registrieren eine Domäne mithilfe von Amazon Route 53 und konfigurieren Amazon Simple Email Service so, dass alle an Ihre Domäne gesendeten E-Mails einem Amazon Simple Storage Service-Bucket zugestellt werden.

Note

Amazon SES unterstützt E-Mail-Empfang nur in bestimmten AWS Regionen. Eine vollständige Liste der Regionen, in denen der E-Mail-Empfang unterstützt wird, finden Sie unter [Amazon Simple Email Service -Endpunkte und -Kontingente](#) in der Allgemeinen AWS Referenz.

Themen

- [Schritt 1: Bevor Sie beginnen](#) (p. 225)
- [Schritt 2: Überprüfen Ihrer Domäne](#) (p. 225)
- [Schritt 3: So richten Sie eine Empfangsregel ein](#) (p. 226)
- [Schritt 4: So senden Sie eine Test-E-Mail](#) (p. 228)
- [Schritt 5: Die empfangene E-Mail anzeigen](#) (p. 229)
- [Schritt 6: Bereinigen](#) (p. 229)

Schritt 1: Bevor Sie beginnen

Bevor Sie mit diesem Tutorial beginnen, melden Sie sich für ein AWS Konto an, sofern Sie noch keines haben, und verwenden Sie [Amazon Route 53](#) um die Domäne zu registrieren, die Sie zum Empfangen von E-Mails verwenden möchten.

Note

Amazon SES unterstützt E-Mail-Empfang nur in bestimmten AWS Regionen. Eine vollständige Liste der Regionen, in denen der E-Mail-Empfang unterstützt wird, finden Sie unter [Amazon Simple Email Service -Endpunkte und -Kontingente](#) in der Allgemeinen AWS Referenz.

Registrieren bei AWS

Wenn Sie bereits über ein AWS Konto verfügen, können Sie diesen Abschnitt überspringen.

So erstellen Sie ein AWS-Konto

1. Wechseln Sie zu <https://console.aws.amazon.com/ses/>. Klicken Sie auf und danach auf **Erste Schritte** mit Amazon SES.
2. Auf der **Erstellen eines AWS-Kontos** Füllen Sie die Pflichtfelder aus und befolgen Sie die Bildschirmanweisungen zum Erstellen eines neuen Kontos.

Registrieren einer Domain mit Route 53

In diesem Tutorial wird davon ausgegangen, dass Sie eine Domäne verwenden, die Sie mithilfe von Route 53 registriert haben. Sie können auch eine Domäne verwenden, die über einen anderen Service registriert wurde. Die Verfahren zum Verifizieren Ihrer Domäne weichen dann aber von den in diesem Tutorial angegebenen Verfahren ab. Weitere Informationen zur Verwendung von Route 53 zum Registrieren einer Domäne finden Sie unter [Registrieren einer neuen Domäne](#) im Entwicklerleitfaden für Amazon Route 53.

Sie können auch eine vorhandene Domäne an Route 53 übertragen. Weitere Informationen zum Übertragen von Domänen an Route 53 finden Sie unter [Übertragen der Registrierung für eine Domäne an Route 53](#) im Entwicklerleitfaden für Amazon Route 53.

Nächster Schritt: [Schritt 2: Überprüfen Ihrer Domäne \(p. 225\)](#)

Schritt 2: Überprüfen Ihrer Domäne

Bevor Sie Amazon SES für den Empfang von E-Mail für Ihre Domäne konfigurieren können, müssen Sie nachweisen, dass sich die Domäne in Ihrem Besitz befindet. Sie können alle Domänen in Ihrem Besitz verifizieren, es ist aber einfacher, Domänen zu verifizieren, die Sie mit Route 53 registriert haben.

Note

Wenn sich Ihr Konto noch in der Amazon SES Sandbox befindet, führen Sie das Verfahren unter [Verlassen der Amazon SES -Sandbox \(p. 79\)](#) bevor Sie das Verfahren in diesem Abschnitt ausführen.

So verifizieren Sie eine Domäne mit Amazon SES

1. Öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.

Note

Um die Schritte in diesem Abschnitt auszuführen, melden Sie sich bei der AWS Management Console mit demselben AWS-Konto an, mit dem Sie Ihre Domäne mit Route 53 registriert haben.

2. Wählen Sie im Navigationsbereich unter Identity Management die Option Domains aus.
3. Wählen Sie Verify a New Domain aus.
4. Auf der So verifizieren Sie eine neue Domäne für-Domäne, geben Sie den Namen der Domäne ein, die Sie mit Route 53 registriert haben, und wählen Sie dann So verifizieren Sie diese Domäne.
5. Auf der So verifizieren Sie eine neue Domäne die Option Verwenden Route 53.

Note

Wenn Sie die Option Verwenden Route 53 ist Ihre Domäne möglicherweise nicht mit Route 53 registriert. Wenn Sie Ihre Domäne mit einem anderen Service registriert haben, können Sie die Domäne nach der Anleitung in [Verifizieren einer Domäne mit Amazon SES \(p. 66\)](#) verifizieren.

6. Wählen Sie im Dialogfeld Use Route 53 (Route 53 verwenden) Domain Verification Record (Domänenverifizierungs-Datensatz) und Email Receiving Record (Empfangsbereite E-Mail für Datensatz) aus. Wählen Sie dann unter Hosted Zones (Gehostete Zonen) die gehostete Zone aus, die Sie verwenden möchten. Wenn Sie an der bei Route 53 registrierten Domäne keine Änderungen vorgenommen haben, sollte in der Gehostete Zonen Abschnitts erstellt.

Important

Wenn Sie bereits Mail-Exchanger (MX)-Datensätze für Ihre Domäne eingerichtet haben, werden diese Datensätze im nächsten Schritt durch die neuen Datensätze ersetzt.

7. Wählen Sie Create Record Sets aus. Sie kehren zur Liste der Domänen zurück.
8. Warten Sie fünf Minuten und klicken Sie dann auf die Schaltfläche refresh (Aktualisieren) (↻). Bestätigen Sie, dass in der Spalte Status der Wert verified (verifiziert) steht. Wenn der Status pending verification (ausstehende Verifizierung) lautet, warten Sie einige Minuten. Aktualisieren Sie die Liste dann erneut. Wiederholen Sie den Vorgang, bis als Domänenstatus verified (verifiziert) angegeben wird.

Nächster Schritt: [Schritt 3: So richten Sie eine Empfangsregel ein \(p. 226\)](#)

Schritt 3: So richten Sie eine Empfangsregel ein

Um Amazon SES als E-Mail-Receiver zu verwenden, müssen Sie über einen aktiven Satz für Empfangsregelsatz. Ein Empfangsregelsatz ist eine Sammlung von Regeln für den Empfang, die festlegen, wie Amazon SES mit E-Mails verfahren soll, die der Service für Ihre verifizierten Domänen empfängt. Da Sie den E-Mail-Empfang mit Amazon SES erstmalig einrichten, erstellt Amazon SES automatisch einen Standard-Empfangsregelsatz für Sie. Die Empfangsregel, die Sie in diesem Abschnitt erstellen, gehört dem Standard-Empfangsregelsatz an.

Note

Die Verfahren in diesem Abschnitt gehen davon aus, dass Sie noch nie einen Empfangsregelsatz erstellt haben. Wenn Ihr Konto bereits eine Empfangsregelsatz enthält, müssen Sie die von Ihnen in diesem Abschnitt erstellte Empfangsregel zuerst aktivieren, bevor Amazon SES sie auf die eingehenden E-Mail für Ihre Domäne anwendet. Weitere Informationen zum Aktivieren und Deaktivieren von Empfangsregeln finden Sie unter [Aktivieren und Deaktivieren eines Empfangsregelsatzes \(p. 253\)](#).

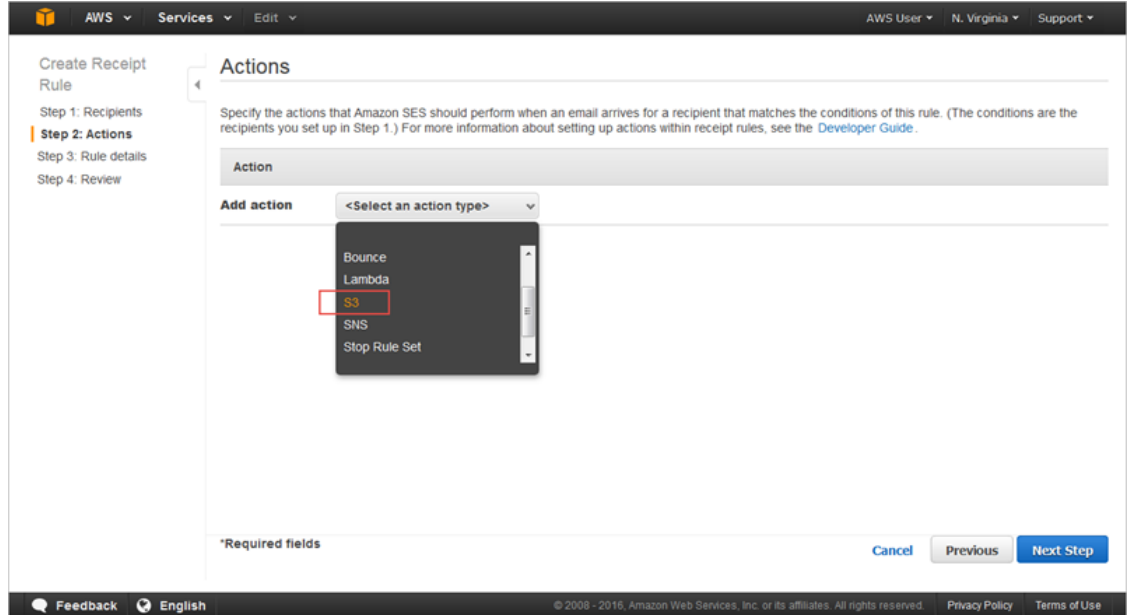
So erstellen Sie eine Empfangsregel

1. Wählen Sie im Navigationsbereich unter Email Receiving (Empfangen von E-Mails) die Option Rule Sets (Regelsätze) aus.
2. Klicken Sie auf Create a Receipt Rule.
3. Klicken Sie auf der Seite Recipients auf Next Step.

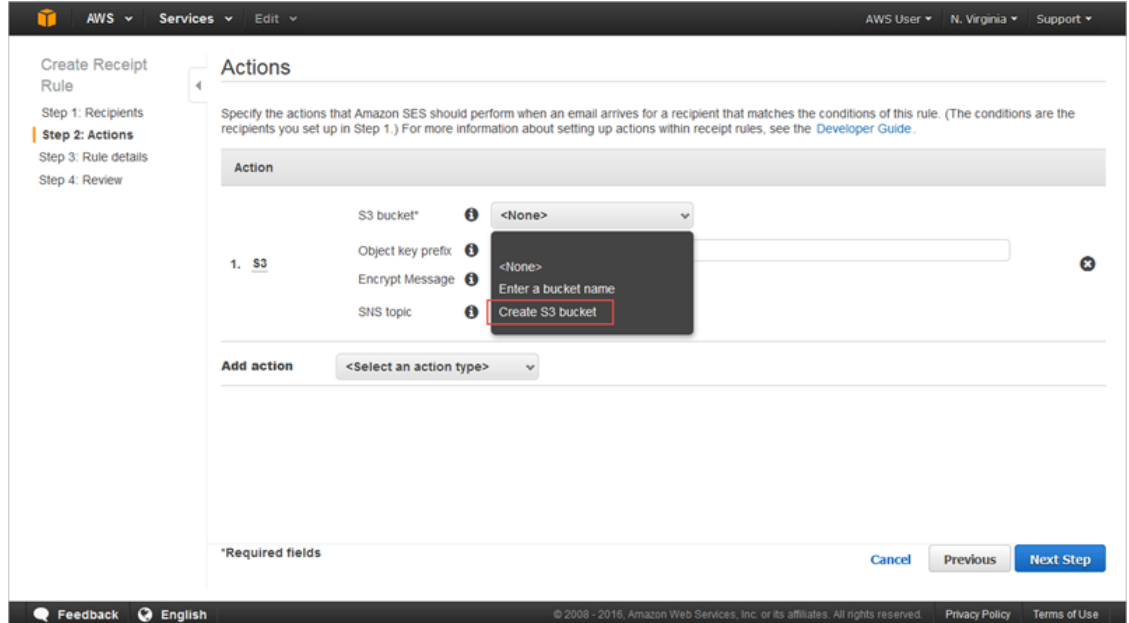
Note

Da Sie keine Empfänger hinzuzufügen, wendet Amazon SES diese Regel auf alle Empfänger in sämtlichen verifizierten Domänen an.

4. Wählen Sie für Add action (Aktion hinzufügen) S3 aus.



5. Wählen Sie für S3 bucket die Option Create S3 bucket aus.



6. Für Bucket-Name einen Namen für den Amazon S3 Bucket ein. Der von Ihnen eingegebene Bucket-Name muss die folgenden Anforderungen erfüllen:
 - Er darf nur Kleinbuchstaben, Zahlen, Punkte (.) und Bindestriche (-) enthalten.
 - Er muss in AWS eindeutig sein.
 - Er muss mit einer Zahl oder einem Kleinbuchstaben beginnen und enden.

- Er muss mindestens 3 und darf höchstens 63 Zeichen umfassen.
- Er darf nicht als IP-Adresse (z. B. 192.168.5.4) formatiert sein.
- Er darf keine zwei aufeinander folgenden Punkte (..) oder einen Bindestrich neben einem Punkt (- oder -) enthalten.

Wenn Sie fertig sind, klicken Sie auf Create Bucket (Bucket erstellen).

Note

Da Sie den Amazon SES-Bucket mithilfe der Amazon S3-Konsole erstellen, erstellt Amazon SES automatisch die Richtlinie, die erforderlich ist, um Schreibberechtigung für diesen Bucket zu erteilen, und wendet sie an. Wenn Sie jedoch einen vorhandenen Amazon S3 Bucket auswählen, müssen Sie Amazon SES die Berechtigung zum Schreiben in diesen Bucket gewähren, indem Sie [Anhängen einer Richtlinie an den Bucket \(p. 235\)](#) mithilfe der Amazon S3 Konsole oder -API.

7. Klicken Sie auf Next Step.
8. Geben Sie auf der Seite Rule Details (Regel-Details) unter Rule name (Regelname) **my-rule** ein. Aktivieren Sie das Kontrollkästchen neben Enabled (Aktiviert) und wählen Sie dann Next Step (Nächster Schritt) aus.

The screenshot shows the 'Rule Details' page in the AWS Management Console. On the left, a sidebar lists the steps: Step 1: Recipients, Step 2: Actions, Step 3: Rule details (highlighted), and Step 4: Review. The main content area is titled 'Rule Details' and includes a sub-header 'Name your rule, and select other options. For more information about receipt rule options, see the [Developer Guide](#).' Below this, there are several sections: 'Rule name*' with a text input containing 'my-rule'; 'Enabled' with a checked checkbox; 'Require TLS' with an unchecked checkbox; 'Enable spam and virus scanning' with a checked checkbox; 'Rule set' with a dropdown menu set to 'default-rule-set' and a 'Create new rule set' link; and 'Rule position' with a dropdown menu set to '<Beginning>'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next Step' (which is highlighted with a red box). The footer of the console shows 'Feedback', 'English', and copyright information for 2008-2016.

9. Wählen Sie auf der Seite Review die Option Create Rule aus.

Nächster Schritt: [Schritt 4: So senden Sie eine Test-E-Mail \(p. 228\)](#)

Schritt 4: So senden Sie eine Test-E-Mail

Nachdem Sie Ihre Domäne verifiziert und konfiguriert haben, können Sie eine E-Mail senden, um die Fähigkeit der Domäne zum Empfangen von E-Mails zu testen.

Senden Sie eine Test-E-Mail von einem E-Mail-Konto, das bekanntlich zum Senden von E-Mails fähig ist, wie z. B. Ihre persönliche E-Mail-Adresse. Senden Sie eine Testnachricht an eine E-Mail-Adresse in Ihrer verifizierten Domäne. Wenn Sie Ihre Domäne beispielsweise example.com lautet, können Sie eine E-Mail an test@example.com oder abc123@example.com (oder eine beliebige andere Adresse in der Domäne example.com) senden.

Note

Sie müssen keine zusätzlichen Schritte ausführen, um in Ihrer Domäne einzelne E-Mail-Adressen zu erstellen. Amazon SES empfängt alle E-Mails, die an beliebige Adressen in der verifizierten Domäne gesendet werden. Dabei wird die von Ihnen in erstellte Empfangsregel angewandt. [Schritt 3: So richten Sie eine Empfangsregel ein \(p. 226\)](#).

Nächster Schritt: [Schritt 5: Die empfangene E-Mail anzeigen \(p. 229\)](#)

Schritt 5: Die empfangene E-Mail anzeigen

Nachdem Sie eine Testnachricht an eine Adresse in Ihrer Domäne gesendet haben, können Sie sie aus Ihrem Amazon S3 Bucket abrufen und ihren Inhalt anzuzeigen.

So zeigen Sie eine über Amazon SES empfangene Nachricht an

1. Öffnen Sie die Amazon S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie in der Amazon S3 Konsole den Bucket aus, den Sie unter [Schritt 3: So richten Sie eine Empfangsregel ein \(p. 226\)](#).
3. Suchen Sie im Amazon S3 Bucket die empfangene E-Mail. Der Name der E-Mail ist eine eindeutige Zeichenfolge aus Buchstaben und Zahlen.

Note

Der Bucket kann außerdem eine Datei namens `AMAZON_SES_SETUP_NOTIFICATION` enthalten. Sie können diese Datei ignorieren oder löschen.

4. Aktivieren Sie das Kontrollkästchen neben dem Namen der Datei. Wählen Sie im Menü Actions die Option Download aus.
5. Öffnen Sie den Ordner auf Ihrem Computer mit der Datei, die Sie im vorhergehenden Schritt heruntergeladen haben. Es gibt mehrere Möglichkeiten, um die heruntergeladene Nachricht einzusehen. Dazu gehören:
 - Öffnen Sie die Datei in einem Texteditor und lesen Sie den Inhalt direkt. Je nach der zum Senden der E-Mail verwendeten Methode, kann ein Teil der Nachricht codiert sein. Wenn die Nachricht teilweise codiert ist, müssen Sie sie manuell decodieren (z. B. mittels eines Base64-Decoders).
 - Fügen Sie die `.eml`-Erweiterung an das Ende der Datei an und öffnen Sie die Datei mithilfe eines E-Mail-Clients wie Microsoft Outlook oder Mozilla Thunderbird. Die meisten E-Mail-Clients decodieren automatisch die codierten Teile der Nachricht und zeigen u. a. HTML-Formatierung und Dateianlagen an.

Nächster Schritt: [Schritt 6: Bereinigen \(p. 229\)](#)

Schritt 6: Bereinigen

Nach Abschluss dieses Tutorials sollten Sie die von Ihnen erstellten Ressourcen bereinigen, um zu vermeiden, dass hierfür zusätzliche Gebühren anfallen.

Amazon SES Empfangsregelsatz

Wenn Amazon SES keine E-Mails mehr für Ihre Domäne empfangen soll, können Sie [So deaktivieren Sie einen aktivierten Empfangsregelsatz \(p. 253\)](#).

Amazon S3 Bucket

Wenn Sie den erstellten Amazon S3 Bucket nicht mehr benötigen, können Sie ihn löschen. Um einen Bucket löschen zu können, müssen Sie zunächst seinen Inhalt löschen. Weitere Informationen zum

Löschen von Ordnern und Buckets finden Sie unter [Objekt und Bucket löschen](#) im Handbuch „Erste Schritte“ für Amazon Simple Storage Service.

Route 53

Wenn Sie Route 53 nicht mehr zur Registrierung Ihrer Domäne nutzen möchten, können Sie [Löschen der Registrierung](#) oder [die Domain an einen anderen Registrar übertragen](#).

Einrichten von Amazon SES E-Mail-Empfang

In diesem Abschnitt wird beschrieben, wie Sie für den Empfang Ihrer E-Mail konfigurieren müssen. Beispielsweise sollten Sie zuerst überlegen, wie Sie Ihre E-Mails erhalten, filtern und verarbeiten möchten, da sich diese Entscheidungen darauf auswirken, wie Sie Amazon SES konfigurieren. Sie müssen darüber hinaus Ihre Domäne bei Amazon SES verifizieren, um ihren Besitz nachzuweisen, und Ihre Domäne anschließend für das Senden eingehender E-Mails an Amazon SES konfigurieren. Als Nächstes erteilen Sie Amazon SES S-Berechtigung, auf AWS Ressourcen zuzugreifen. Zuletzt konfigurieren Sie den E-Mail-Empfang, indem Sie einen Empfangsregelsatz, Empfangsregeln und IP-Adressenfilter erstellen.

Diese Schritte werden in den folgenden Themen beschrieben:

- [Berücksichtigen Sie Ihren Anwendungsfall für Amazon SES E-Mail-Empfang \(p. 230\)](#)
- [Bestätigen Sie Ihre Domain für Amazon SES E-Mail-Empfang \(p. 232\)](#)
- [Veröffentlichen eines MX-Eintrags für Amazon SES E-Mail-Empfang \(p. 233\)](#)
- [Erteilen von Berechtigungen für Amazon SES für den E-Mail-Empfang \(p. 235\)](#)
- [Erstellen von IP-Adressfiltern für Amazon SES E-Mail-Empfang \(p. 238\)](#)
- [Erstellen eines Wareneingangsregelsatzes für Amazon SES E-Mail-Empfang \(p. 238\)](#)
- [Erstellen von Zahlungsregeln für Amazon SES E-Mail-Empfang \(p. 239\)](#)

Informationen dazu, an welchem Punkt des E-Mail-Empfangsprozesses diese Aufgaben ausgeführt werden, finden Sie unter [Konzepte für den E-Mail-Empfang \(p. 222\)](#).

Berücksichtigen Sie Ihren Anwendungsfall für Amazon SES E-Mail-Empfang

Bevor Sie Amazon SES für den Empfang Ihrer E-Mail einrichten, sollten Sie sich folgende Fragen stellen.

Allgemeine Überlegungen

Befindet sich Ihr Amazon SES Konto noch in der Sandbox?

Wenn Sie dies noch nicht getan haben, führen das Verfahren unter [Verlassen der Amazon SES - Sandbox \(p. 79\)](#) Damit Ihr Konto aus der Amazon SES -Sandbox entfernt werden kann.

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 angegebenen 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 im Format Multipurpose Internet Mail Extensions (MIME) zu. Weitere Informationen zum MIME-Format finden Sie unter [RFC 2045](#).

Wie groß sind die E-Mails, die Sie erhalten werden?

Wenn Sie E-Mails in einem Amazon S3 Bucket speichern, beträgt die maximale E-Mail-Größe (einschließlich Header) 30 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 an 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 zu AWS Lambda finden Sie im [Developer-Handbuch für AWS Lambda](#).

- 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 kann in integriert werdenAWS Key Management Service(AWS KMS) können Sie die E-Mails, die in Ihren Amazon S3 Bucket geschrieben werden, optional verschlüsseln. 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 Ihrer Seite entschlüsseln müssen, nachdem Sie die E-Mail von Amazon S3 abgerufen haben. [AWS SDK for Java](#) und [AWS SDK for Ruby](#) stellen einen Client bereit, der die Entschlüsselung für Sie übernehmen kann. Amazon SES kann die E-Mails für Sie nur entschlüsseln, wenn Sie Ihre E-Mail-Nachrichten einem Amazon S3 Bucket zugestellt werden.

Unerwünscht

An welchem Punkt des E-Mail-Empfangsprozesses möchten Sie unerwünschte E-Mails ablehnen?

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 ablehnen – während der SMTP-Aushandlung und nach der SMTP-Aushandlung. Verwenden Sie IP-Adressenfilter, um Nachrichten während der SMTP-Aushandlung abzulehnen, und Empfangsregeln, um E-Mails nach der SMTP-Aushandlung abzulehnen.

Mit IP-Adressenfiltern können Sie E-Mails ablehnen, die von bestimmten IP-Adressen stammen. Das Ablehnen unerwünschter E-Mails mit Hilfe von IP-Adressenfiltern hat den Vorteil, dass für Nachrichten,

die während der SMTP-Aushandlung abgelehnt 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 abgelehnt werden. Weitere Informationen zu IP-Adressfiltern finden Sie unter [Erstellen von IP-Adressfiltern für Amazon SES E-Mail-Empfang](#) (p. 238).

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. So können Sie beispielsweise AWS Lambda verwenden, um nur dann eine Unzustellbarkeitsbenachrichtigung zu senden, wenn die DKIM-Authentifizierung für eine Nachricht fehlschlägt oder sie als Spam eingestuft wird. 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 [Erstellen von Zahlungsregeln für Amazon SES E-Mail-Empfang](#) (p. 239). Weitere Informationen zur Verwendung von Lambda für die Analyse eingehender E-Mails finden Sie unter [Lambda -Funktion](#) (p. 247).

Verwenden von anderen AWS -Services

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 Mastermaster verwenden, müssen Sie Amazon SES die Berechtigung erteilen, um auf diese Ressourcen zuzugreifen. Um Amazon SES den Zugriff zu erteilen, erstellen Sie Richtlinien für die Ressourcen über die Konsolen oder APIs dieser AWS -Services. Weitere Informationen finden Sie unter [Erteilen einer Erlaubnis](#) (p. 235).

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](#) (p. 239).

Regionale Verfügbarkeit

Unterstützt Amazon SES den Empfang von E-Mails in Ihrer Region?

Amazon SES unterstützt nur E-Mail-Empfang in bestimmten AWS Regionen. Eine vollständige Liste der Regionen, in denen der E-Mail-Empfang unterstützt wird, finden Sie unter [Amazon Simple Email Service-Endpunkte und -Kontingente](#). Sie finden in der Allgemeinen AWS Referenz.

Bestätigen Sie Ihre Domain für 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 Amazon SES und

die anschließende Veröffentlichung eines TXT-Datensatzes auf Ihrem DNS-Server umfasst, wird unter [Überprüfen von Domänen in Amazon SES \(p. 65\)](#).

Note

Obwohl Amazon SES Ihnen ermöglicht, einzelne E-Mail-Adressen zu bestätigen, müssen Sie eine Domäne verifizieren, wenn Sie Amazon SES für den E-Mail-Empfang verwenden möchten.

Sie können den Domänenverifizierungsprozess auch starten, wenn Sie die Empfangsregeln in [Erstellen von Empfangsregeln \(p. 239\)](#) einrichten. Die Empfängerliste gibt an, welche Empfänger nicht verifiziert sind, und ermöglicht Ihnen, die Verifizierung zu initiieren. In jedem Fall müssen Sie die Domänenverifizierung abschließen, indem Sie einen TXT-Datensatz auf Ihrem DNS-Server veröffentlichen, wie unter [TXT-Datensätze zur Amazon SES E-Domänenverifizierung \(p. 69\)](#) beschrieben.

Sie können nachsehen, ob Ihre E-Mail-Adresse oder Domäne verifiziert wurde, indem Sie deren Status in der Listidentitäten von E-Mail-Adressen oder .Domain-Identitäten in der Amazon SES Konsole oder mithilfe der Amazon SES `GetIdentityVerificationAttributes`-API.

Veröffentlichen eines MX-Eintrags für 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.

Um Ihre eingehenden E-Mails von Amazon SES zu verwalten, müssen Sie zur DNS-Konfiguration Ihrer Domäne einen MX-Datensatz hinzufügen. Der von Ihnen erstellte MX-Datensatz verweist 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 beispielsweise `inbound-smtp.us-west-2.amazonaws.com`. Eine vollständige Liste der Endpunkte finden Sie unter [Amazon SES Regionen und -Endpunkte \(p. 494\)](#).

Note

Die Endpunkte, die E-Mails in Amazon SES empfangen, sind keine IMAP- oder POP3-E-Mail-Server. Es ist nicht möglich, diese URLs als Posteingangsserver in E-Mail-Clients zu verwenden. Wenn Sie eine Lösung benötigen, mit der sich E-Mails über einen E-Mail-Client senden und empfangen lassen, können Sie verwenden [Amazon WorkMail](#).

Das folgende Verfahren enthält allgemeine Schritte zum Erstellen eines MX-Datensatzes. Das spezifische Verfahren für das Erstellen eines MX-Datensatzes hängt 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

Damit Sie folgenden Schritte ausführen können, müssen Sie berechtigt sein, die DNS-Datensätze für Ihre Domäne zu ändern. Wenn Sie keinen Zugriff auf die DNS-Datensätze für Ihre Domäne haben oder diese nicht bearbeiten möchten, wenden Sie sich für Unterstützung an Ihren Systemadministrator.

So fügen Sie einen MX-Datensatz zur DNS-Konfiguration für Ihre Domäne hinzu:

1. Melden Sie sich bei der Managementkonsole für Ihren DNS-Anbieter an.
2. Erstellen Sie einen neuen MX-Datensatz.
3. Für den MX-DatensatzNameGeben Sie Ihre Domain ein, gefolgt von einem Punkt. Wenn Sie möchten, dass Amazon SES E-Mails verwaltet, die an die Domäne gesendet werden, geben Sie Folgendes ein:

```
example.com.
```

Note

Bei einigen DNS-Anbietern wird das Feld Name als Host, Domäne oder Maildomäne bezeichnet.

4. Wählen Sie für Type (Typ) die Option MX aus.

Note

Bei einigen DNS-Anbietern wird das Feld Type (Typ) als Datensatztyp oder so ähnlich bezeichnet.

5. Geben Sie für Value (Wert) Folgendes ein:

```
10 inbound-smtp.regionInboundUrl.amazonaws.com
```

Ersetzen Sie im obigen Beispiel *RegionInboundUrl* mit der 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, ersetzen Sie *region* mit *us-east-1*. Eine Liste aller Endpunkte für den E-Mail-Empfang finden Sie unter [Amazon SES Regionen und -Endpunkte \(p. 494\)](#).

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.

Anleitung 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
GoDaddy	Hinzufügen eines MX-Datensatzes
DreamHost	Wie ändere ich meine MX-Datensätze?
Cloudflare	Wie kann ich Mail- oder MX-Datensätze hinzufügen oder bearbeiten?
HostGator	Ändern von MX-Datensätzen — Windows
Namecheap	Wie kann ich die für den Mail-Service benötigten MX-Datensätze einrichten?
Names.co.uk	Ändern der DNS-Einstellungen Ihrer Domäne

Name des DNS/Hosting-Anbieters	Link zur Dokumentation
Wix	Hinzufügen oder Aktualisieren von MX-Datensätzen in Ihrem Wix-Konto

Erteilen von Berechtigungen für Amazon SES für den E-Mail-Empfang

Einige der Aufgaben, die Sie ausführen können, wenn Sie E-Mails in Amazon SES erhalten, z. B. das Senden von E-Mails an einen Amazon S3 Bucket oder das Aufrufen einer Lambda Funktion, erfordern besondere Berechtigungen. Dieser Abschnitt enthält Richtlinienbeispiele für einige allgemeine - Anwendungsfälle.

Themen in diesem Abschnitt:

- [Erteilen Sie Amazon SES die Berechtigung zum Schreiben in einen Amazon S3 Bucket \(p. 235\)](#)
- [Erteilen Sie Amazon SES die Berechtigung, Ihre AWS KMS Masterschlüssel \(p. 236\)](#)
- [Erteilen Sie Amazon SES die Berechtigung zum Aufrufen einer Lambda -Funktion \(p. 237\)](#)
- [Erteilen Sie Amazon SES die Berechtigung zum Veröffentlichen in ein Amazon SNS -Thema, das einem anderen AWS Konto gehört. \(p. 237\)](#)

Erteilen Sie Amazon SES die Berechtigung zum Schreiben in einen Amazon S3 Bucket

Wenn Sie die folgende Richtlinie auf einen Amazon S3 Bucket anwenden, erteilt Amazon SES die Berechtigung zum Schreiben von Daten in diesen Bucket. Weitere Informationen zum Erstellen von Empfangsregeln, die eingehende E-Mails an Amazon S3 übertragen, finden Sie unter [S3-Aktion \(p. 250\)](#).

Weitere Informationen zum Anfügen von Richtlinien an Amazon S3 Buckets finden Sie unter [Verwendung von Bucket-Richtlinien und Benutzerrichtlinien](#) im Amazon Simple Storage Service – Entwicklerhandbuch.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSESPuts",
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::myBucket/*",
      "Condition": {
        "StringEquals": {
          "aws:Referer": "111122223333"
        }
      }
    }
  ]
}
```

Nehmen Sie die folgenden Änderungen am vorhergehenden Richtlinienbeispiel vor:

- Ersetzen **MyBucket** mit dem Namen des Amazon S3 Buckets, in den Sie schreiben möchten.

- Ersetzen **111122223333** Sie können Ihre AWS Konto-ID angeben.

Erteilen Sie Amazon SES die Berechtigung, Ihre AWS KMS Masterschlüssel

Damit Amazon SES Ihre E-Mails verschlüsseln kann, ist die Berechtigung zur Verwendung der AWS KMS-Taste, den Sie beim Einrichten der Empfangsregel angegeben haben. Sie können entweder den Standardmasterschlüssel (aws/ses) in Ihrem Konto oder verwenden Sie einen benutzerdefinierten Masterschlüssel, den Sie erstellen. Wenn Sie den Standardmasterschlüssel verwenden, brauchen Sie keine zusätzlichen Schritte ausführen, um Amazon SES die Berechtigung zur Verwendung des Schlüssels zu erteilen. Wenn Sie einen benutzerdefinierten Masterschlüssel verwenden, müssen Sie Amazon SES die entsprechende Berechtigung erteilen, indem Sie der Richtlinie des Schlüssels eine Anweisung hinzufügen.

Um Amazon SES die folgende Richtlinienanweisung als Schlüsselrichtlinie zu verwenden, um Amazon SES zu erlauben, Ihren benutzerdefinierten Masterschlüssel zu verwenden, wenn er E-Mails in Ihrer Domäne empfängt.

```
{
  "Sid": "AllowSESToEncryptMessagesBelongingToThisAccount",
  "Effect": "Allow",
  "Principal": {
    "Service": "ses.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

Note

Amazon SES verwendet Amazon S3 [Mehrteiliger Upload API](#), um große Nachrichten (5 MB oder größer) an Amazon S3 Buckets zu senden. Wenn Sie AWS KMS Wenn Sie verschlüsselte Nachrichten an einen Amazon S3 Bucket senden und möchten, Nachrichten empfangen möchten, die größer als 5 MB sind, sollten Sie anstelle der Anweisung im vorherigen Beispiel die folgende Richtlinienanweisung verwenden:

```
{
  "Sid": "AllowSESToEncryptMessagesBelongingToThisAccount",
  "Effect": "Allow",
  "Principal": {
    "Service": "ses.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Weitere Informationen zu Multipart-Uploads in Amazon S3 finden Sie unter [Multipart-Upload-API und Berechtigungen](#) im Amazon Simple Storage Service – Entwicklerhandbuch. Weitere Informationen zum Anfügen von Richtlinien an AWS KMS Tasten finden Sie unter [Verwenden von Schlüsselrichtlinien in AWS KMS](#) im AWS Key Management Service Entwicklerhandbuch.

Erteilen Sie Amazon SES die Berechtigung zum Aufrufen einer Lambda -Funktion

Damit Amazon SES eine Lambda Funktion aufrufen kann, können Sie die Funktion auswählen, wenn Sie eine Zahlungsregel in der Amazon SES Konsole erstellen. Wenn Sie dies tun, fügt Amazon SES automatisch die erforderlichen Berechtigungen zur -Funktion hinzu.

Sie können aber auch die `AddPermission`-Operation im AWS Lambda-API verwenden, um eine Richtlinie einer Funktion zuzuordnen. Der folgende Aufruf der `AddPermission`-API gewährt Amazon SES die Berechtigung zum Aufrufen Ihrer Lambda -Funktion. Ersetzen Sie im folgenden Beispiel `111122223333` Sie können Ihre AWS Konto-ID angeben. Weitere Informationen zum Anfügen von Richtlinien an Lambda Funktionen finden Sie unter [AWS Lambda Berechtigungen](#) im AWS Lambda Entwicklerhandbuch.

```
{
  "Action": "lambda:InvokeFunction",
  "Principal": "ses.amazonaws.com",
  "SourceAccount": "111122223333",
  "StatementId": "GiveSESPermissionToInvokeFunction"
}
```

Erteilen Sie Amazon SES die Berechtigung zum Veröffentlichen in ein Amazon SNS -Thema, das einem anderen AWS Konto gehört.

Wenn das Amazon SNS -Thema, das Sie verwenden möchten, demselben AWS Konto gehört, das Sie für Amazon SES verwenden, kann Amazon SES dieses Thema ohne zusätzliche Einrichtungsschritte veröffentlichen. Wenn Sie Benachrichtigungen in einem separaten AWS Konto in einem -Thema veröffentlichen möchten, müssen Sie dem Amazon SNS eine Richtlinie anfügen.

Die folgenden Richtlinie erteilt Amazon SES die Berechtigung zum Veröffentlichen in einem Amazon SNS -Thema in einem separaten AWS Konto.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:SNS-TOPIC-ACCOUNT-ID:myTopic",
      "Condition": {
        "StringEquals": {
          "AWS:SourceOwner": "SES-RECEIVING-ACCOUNT-ID"
        }
      }
    }
  ]
}
```

Nehmen Sie die folgenden Änderungen am vorhergehenden Richtlinienbeispiel vor:

- Ersetzen `us-west-2` Mit der AWS Region, in der sich das Amazon SNS -Themas befindet.
- Ersetzen `SNS-TOPIC-ACCOUNT-ID` mit der ID des AWS Kontos, in dem sich das Amazon SNS Topic befindet.

- Ersetzen **MyTopic** mit dem Namen des Amazon SNS Topics, für das Sie Benachrichtigungen veröffentlichen möchten.
- Ersetzen **SES-EMPFANGEN-ACCOUNT-ID** mit der ID des AWS Kontos, das für den E-Mail-Empfang konfiguriert ist.

Erstellen von IP-Adressfiltern für Amazon SES E-Mail-Empfang

Mithilfe eines IP-Adressenfilters können Sie optional angeben, ob E-Mails, die von einer IP-Adresse oder aus einem IP-Adressbereich stammen, akzeptiert oder abgelehnt werden sollen.

Sie können die Amazon SES Konsole oder die `CreateReceiptFilter`-API zum Erstellen eines IP-Adressfilters.

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 vertrauen. Diese Konfiguration blockiert alle IP-Adressen standardmäßig und lässt nur E-Mails von den IP-Adressen zu, die Sie explizit angeben.

So erstellen Sie einen IP-Adressenfilter (Konsole)

1. Melden Sie sich beim `an.AWS Management Console` und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option IP Address Filters aus.
3. Wählen Sie im Inhaltsbereich die Option Create Filter aus.
4. Geben Sie für Filter Name einen Namen für den IP-Adressenfilter ein. Der Name muss weniger als 64 alphanumerische Zeichen, Bindestriche (-), Unterstriche (_), Punkte (.) enthalten. Der Name muss mit einem Buchstaben oder einer Zahl beginnen.
5. Geben Sie für IP Address Range eine einzelne IP-Adresse oder einen IP-Adressenbereich ein, den Sie blockieren oder zulassen möchten, und verwenden Sie dabei die Classless Inter-Domain Routing (CIDR)-Notation. 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 unter [RFC 2317](#).
6. Wählen Sie für Policy Type die Option Allow oder Block aus.
7. Wählen Sie Create Filter.

Weitere Informationen zur Verwendung des `CreateReceiptFilter`-API zum Erstellen eines IP-Adressenfilters finden Sie im [Amazon Simple Email Service API-Referenz](#).

Erstellen eines Wareneingangsregelsatzes für Amazon SES E-Mail-Empfang

Ein Empfangsregelsatz ist eine sortierte Sammlung von Empfangsregeln, die festlegen, wie Amazon SES mit E-Mails verfahren soll, die der Service für jede Ihrer Domänen empfängt. Um Amazon SES als E-Mail-Receiver zu verwenden, müssen Sie einen Empfangsregelsatz für Ihr Konto erstellen. Weitere Informationen über die Rolle der Empfangsregelsätze beim E-Mail-Empfang finden Sie unter [Konzepte für den E-Mail-Empfang](#) (p. 222).

Nur ein Empfangsregelsatz kann jeweils aktiv sein. Sie können jedoch mehrere Empfangsregelsätze erstellen. Mehrere Empfangsregelsätze können beispielsweise hilfreich sein, wenn Sie die in der

Vergangenheit verwendeten Empfangsregelsätze dokumentieren möchten oder wenn Sie Empfangsregeln für Testzwecke schnell ändern müssen.

Note

Wenn Sie Amazon SES nicht als E-Mail-Receiver verwenden möchten, deaktivieren Sie einfach alle Ihre Empfangsregelsätze. Weitere Informationen zum Deaktivieren von Empfangsregelsätzen finden Sie unter [Verwalten von Empfangsregelsätzen \(p. 253\)](#).

Sie können die Amazon SES Konsole oder die API verwenden, um einen Empfangsregelsatz zu erstellen.

- Verwenden der Amazon SES Konsole
 - Empfangsregeln liegen nur in Empfangsregelsätzen vor. Um einen Empfangsregelsatz zu erstellen, können Sie zunächst eine Empfangsregel festlegen. Weitere Informationen finden Sie unter [Erstellen von Empfangsregeln \(p. 239\)](#). Am Ende dieses Verfahrens können Sie einen neuen Empfangsregelsatz erstellen.
 - Kopieren Sie einen vorhandenen Empfangsregelsatz, wie unter [Verwalten von Empfangsregelsätzen \(p. 253\)](#) beschrieben.
 - Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets und dann Create a New Rule Set aus.
- Verwenden der Amazon SES S-API—Verwenden der `CreateReceiptRuleSet`-API zum Erstellen eines leeren Empfangsregelsatzes, wie im beschrieben [Amazon Simple Email Service API-Referenz](#). Anschließend können Sie die Amazon SES Konsole oder die `CreateReceiptRule`-API verwenden, um Empfangsregeln hinzuzufügen.

Erstellen von Zahlungsregeln für Amazon SES E-Mail-Empfang

Mithilfe von Empfangsregeln können Sie angeben, wie Amazon SES mit E-Mails verfährt, die für die E-Mail-Adressen oder Domänen, die Sie besitzen, empfangen werden. Eine Empfangsregel enthält eine Bedingung und eine sortierte Liste mit Aktionen. Wenn der Empfänger einer eingehenden E-Mail mit einem Empfänger übereinstimmt, der in den Bedingungen für die Empfangsregel festgelegt ist, dann führt Amazon SES die in der Empfangsregel festgelegten Aktionen aus. Weitere Informationen über die Rolle der Empfangsregeln beim E-Mail-Empfang finden Sie unter [Konzepte für den E-Mail-Empfang \(p. 222\)](#).

Important

Zum Einrichten von Empfangsregeln verifizieren Sie zunächst eine Domäne und veröffentlichen einen MX-Datensatz für diese Domäne. Weitere Informationen zum Verifizieren von Domänen finden Sie unter [Überprüfen von Domänen in Amazon SES \(p. 65\)](#). Weitere Informationen zum Veröffentlichen von MX-Datensätzen finden Sie unter [the section called "Veröffentlichen eines MX-Datensatzes" \(p. 233\)](#).

Sie können die Amazon SES Konsole oder den `CreateReceiptRuleSet` erstellen Sie Empfangsregeln. Dieser Abschnitt enthält Verfahren zum Erstellen einer neuen Empfangsregel mithilfe der Konsole. Diese Verfahren setzen voraus, dass Ihr Amazon SES Konto noch keine Empfangsregeln enthält.

So richten Sie eine Empfangsregel

Sie können die Amazon SES Konsole oder den `CreateReceiptRule`-API, um Regeln zu erstellen.

So erstellen Sie eine Empfangsregel mithilfe der Konsole

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.

3. Klicken Sie auf Create a Receipt Rule.
4. Führen Sie die folgenden Schritte aus, um einen oder mehrere Empfänger hinzuzufügen. Gemeinsam bilden diese Empfänger die Bedingung. Sie können maximal 100 Empfänger pro Empfangsregel hinzufügen.
 - a. Geben Sie unter Recipients die eingehende E-Mail-Adresse oder Domäne an, für die Sie eine Empfangsregel einrichten 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.	<code>user@example.com</code>	Es werden auch Varianten der Adresse zugeordnet, die Labels enthalten (z. B. <code>user+123@example.com</code> und <code>user+xyz@example.com</code>). 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.	<code>example.com</code>	
Ordnen Sie alle Adressen innerhalb einer bestimmten Subdomäne zu, jedoch nicht diejenigen in der übergeordneten Domäne.	<code>subdomain.example.com</code>	
Ordnen Sie alle Adressen innerhalb aller Subdomänen zu, jedoch nicht diejenigen in der übergeordneten Domäne.	<code>.example.com</code>	Beachten Sie den Punkt (.) vor dem Domännennamen.
Ordnen Sie alle Adressen innerhalb einer Domäne und alle Adressen in allen Subdomänen zu.	<code>example.com</code> <code>.example.com</code>	Erstellen Sie zwei separate Empfänger: einen mit dem Domännennamen und einen mit einem Punkt gefolgt vom Domännennamen.
Zuordnen aller Empfänger in allen verifizierten Domänen	[Keine]	Lassen Sie das Empfängerfeld 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. Wählen Sie Add Recipient aus.
 - c. Wiederholen Sie die Schritte a und b für jeden Empfänger, den Sie hinzufügen möchten. Wenn Sie alle Empfänger hinzugefügt haben, wählen Sie Next Step aus.
5. Führen Sie die folgenden Schritte aus, um der Empfangsregel eine oder mehrere Aktionen hinzuzufügen.
 - a. Wählen Sie eine Aktion aus dem Menü aus.
 - b. Wählen Sie die Aktionseinstellungen aus. Weitere Informationen zu den Optionen für die einzelnen Aktionen finden Sie unter [Aktionsoptionen](#) (p. 241).
 - c. Fügen Sie zusätzliche Aktionen nach Bedarf hinzu und klicken Sie dann auf Next Step.
6. Verwenden Sie für Rule Details das folgende Verfahren zum Auswählen der Einstellungen.
 - a. Geben Sie unter Rule Name einen Namen für die Empfangsregel ein. Der Name muss weniger als 64 alphanumerische Zeichen, Bindestriche (-), Unterstriche (_), Punkte (.) enthalten. Der Name muss mit einem Buchstaben oder einer Zahl beginnen.
 - b. Wenn Sie die Empfangsregel aktivieren möchten, lassen Sie die Option Enabled ausgewählt.
 - c. Wenn Sie möchten, dass Amazon SES alle eingehenden E-Mails ablehnt, die nicht über eine mit Transport Layer Security (TLS) verschlüsselte Verbindung gesendet werden, wählen Sie TLS.
 - d. Wenn Sie möchten, dass Amazon SES eingehende E-Mails auf Spam und Viren überprüft, wählen Sie Spam- und Virensuche aktivieren.
7. Wählen Sie für Rule Set einen vorhandenen Empfangsregelsatz aus oder klicken Sie auf Create New Rule Set.
8. Wählen Sie für Rule Position die Position aus, an der die Empfangsregel in der sortierten Liste von Empfangsregeln platziert werden soll. Die Empfangsregeln werden nacheinander ausgewertet.
9. Wählen Sie Next Step und anschließend Create Rule aus.

Weitere Informationen zur Verwendung des `CreateReceiptRule`-API zum Erstellen von Regeln finden Sie im [Amazon Simple Email Service API-Referenz](#).

Aktionsoptionen

Jede Empfangsregel für den Amazon SES E-Mail-Empfang enthält eine geordnete Liste der Aktionen. Die gesamte Einrichtung von Empfangsregeln wird unter [Erstellen von Zahlungsregeln für Amazon SES E-Mail-Empfang](#) (p. 239) beschrieben. In diesem Abschnitt werden die spezifischen Optionen für jeden Aktionstyp beschrieben.

Es stehen folgende Aktionstypen zur Verfügung:

- [Aktion „Add header“](#) (p. 242)
- [„Bounce“-Aktion](#) (p. 242)
- [Lambda-Aktion](#) (p. 242)
- [S3-Aktion](#) (p. 250)
- [SNS-Aktion](#) (p. 251)
- [Stop-Aktion](#) (p. 251)
- [WorkMail Aktion](#) (p. 252)

Aktion „Add header“

Mit der Add Header-Aktion 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-Wert**Der Wert des hinzuzufügenden Headers. Er muss kleiner als 2048 Zeichen sein und darf kein Zeilenumbruchzeichen ("r" oder "n") enthalten.

„Bounce“-Aktion

Die 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.
- **Antwort-Absender**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.
- **SNS-Thema-Programm**Der Name oder ARN des Amazon SNS -Themas, der optional benachrichtigt werden soll, wenn eine Unzustellbarkeits-E-Mail gesendet wird. Ein ARN eines Amazon SNS -Themas ist beispielsweise:arn:sns:us-west-2:123456789012:MyTopic. Sie können ein Amazon SNS Topic auch beim Einrichten Ihrer Aktion erstellen, indem Sie Erstellen eines SNS-Themas. Weitere Informationen zu Amazon SNS -Themen finden Sie im [Amazon Simple Notification Service-Entwicklerhandbuch](#).

Note

Das Amazon SNS -Thema, das Sie auswählen, muss sich in derselben AWS Region wie der Amazon SES S-Endpoint befinden, den Sie zum Empfangen von E-Mails 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
- **Postfachvollständig** – 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](#).

Lambda-Aktion

Die Lambda Aktion ruft Ihren Code über eine Lambda Funktion auf und benachrichtigt Sie optional über Amazon SNS. Diese Aktion umfasst die folgenden Optionen.

- **Lambda Funktion**ARN der Lambda-Funktion. Ein Beispiel für eine Lambda ARN ist Arn:EWS:Lambda:us-west-2:Konto-ID:Funktion:MyFunction. Informationen zu AWS Lambda finden Sie im [AWS Lambda-Developer-Handbuch](#).

- **Aufruftyp** Der Aufruftyp der Lambda -Funktion. Der Aufruftyp `RequestResponse` bedeutet, dass die Ausführung der Funktion sofort zu einer Antwort führt, und der Wert `Event` bedeutet, dass die Funktion asynchron aufgerufen wird. Wir empfehlen, den Aufruftyp `Event` zu verwenden, es sei denn, für Ihren Anwendungsfall ist die synchrone Ausführung unbedingt notwendig.

Note

Für den Aufruf von `RequestResponse` gibt es eine Zeitverzögerung von 30 Sekunden.

Weitere Informationen zu AWS Lambda Weitere Informationen zu [AWS Lambda Entwicklerhandbuch](#).

- **SNS-Thema-Programm** Der Name oder ARN des Amazon SNS -Themas, das benachrichtigt werden soll, wenn die angegebene Lambda Funktion ausgelöst wird. Ein ARN eines Amazon SNS -Themas ist beispielsweise: `arn:sns:us-west-2:123456789012:MyTopic`. Sie können ein Amazon SNS Topic auch beim Einrichten Ihrer Aktion erstellen, indem Sie Erstellen eines SNS-Themas. Weitere Informationen zu Amazon SNS -Themen finden Sie im [Amazon Simple Notification Service-Entwicklerhandbuch](#).

Note

Das Amazon SNS -Thema, das Sie auswählen, muss sich in derselben AWS Region wie der Amazon SES S-Endpunkt befinden, den Sie zum Empfangen von E-Mails verwenden.

Schreiben Ihrer Lambda -Funktion

Um Ihre E-Mail zu verarbeiten, 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 die Metadaten auch für den Zugriff auf den Nachrichteninhalte aus Ihrem Amazon S3 Bucket verwenden.

Wenn Sie den Nachrichtenfluss tatsächlich steuern 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: Das erste Argument ist `null` und das zweite Argument ist eine `disposition`-Eigenschaft, die entweder `STOP_RULE`, `STOP_RULE_SET`, oder `CONTINUE`. 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 unter [Lambda -Funktion \(p. 247\)](#). Beispiele für allgemeine Anwendungsfälle finden Sie unter [Anwendungsfälle \(p. 244\)](#).

Format der Eingabedaten

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. Dieses Objekt enthält `receipt` und `mail`-Objekte, die das gleiche Format wie die in beschriebenen Amazon SNS Benachrichtigungen aufweisen. [Inhalte von Benachrichtigungen \(p. 260\)](#).

Note

Die Daten, die Amazon SES an Lambda übergibt, enthalten Metadaten über die Nachricht sowie mehrere E-Mail-Header. Es enthält 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>
        }
      }
    }
  ]
}
```

Return values

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.

Anwendungsfallbeispiele

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: Spam über alle Domänen hinweg ablegen

In diesem Beispiel wird eine globale Regel dargestellt, die Spam-Nachrichten in allen Ihren Domänen löscht. Die Regeln 2 und 3 sollen demonstrieren, dass 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 [Lambda -Funktion \(p. 247\)](#).

Regel 2

Empfängerliste: example1.com

Aktionen

1. Jede beliebige Aktion

Regel 3

Empfängerliste: example2.com

Aktionen

1. Jede beliebige Aktion

Anwendungsfall 2: Spam über alle Domains hinweg ablehnen

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, dass 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: Protokollieren von E-Mail-Ereignissen 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 Lambda Funktionen in [Lambda -Funktion \(p. 247\)](#) Melden Sie sich bei CloudWatch an.
2. S3-Aktion

Anwendungsfall 5: Löscht E-Mails, die DKIM fehlschlagen

In diesem Beispiel wird gezeigt, 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: Filtert E-Mails basierend auf 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.

Lambda -Funktion

Dieses Thema enthält Beispiele für Lambda Funktionen, die den Nachrichtenfluss kontrollieren.

Beispiel 1: Spam löschen

Dieses Beispiel stoppt die Verarbeitung von Nachrichten mit mindestens einem Spam-Indikator.

```
exports.handler = function(event, context, callback) {
    console.log('Spam filter');

    var 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, null);
    }
};
```

Beispiel 2: Fahren Sie fort, 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.

```
exports.handler = function(event, context, callback) {
    console.log('Header matcher');

    var sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

    // Iterate over the headers
    for (var index in sesNotification.mail.headers) {
        var 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, null);
            return;
        }
    }

    // Stop processing the rule if the header value wasn't found
    callback(null, {'disposition':'STOP_RULE'});
};
```

Beispiel 3: Abrufen von E-Mails 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 an Amazon S3 schreiben.

```
var AWS = require('aws-sdk');
var s3 = new AWS.S3();

var bucketName = '<YOUR BUCKET GOES HERE>';

exports.handler = function(event, context, callback) {
    console.log('Process email');

    var sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

    // Retrieve the email from your bucket
    s3.getObject({
        Bucket: bucketName,
        Key: sesNotification.mail.messageId
    }, function(err, data) {
        if (err) {
            console.log(err, err.stack);
            callback(err);
        } else {
            console.log("Raw email:\n" + data.Body);

            // Custom email processing goes here

            callback(null, null);
        }
    });
};
```

Beispiel 4: Bounce-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.

```
'use strict';

const AWS = require('aws-sdk');

// Assign the emailDomain environment variable to a constant.
const emailDomain = process.env.emailDomain;

exports.handler = (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));
  // Try to send the bounce.
  new AWS.SES().sendBounce(sendBounceParams, (err, data) => {
    // If something goes wrong, log the issue.
    if (err) {
      console.log(`An error occurred while sending bounce for message:
${messageId}`, err);
      callback(err);
    } else {
      // Otherwise, log the message ID for the bounce email.
      console.log(`Bounce for message ${messageId} sent, bounce message ID:
${data.MessageId}`);
      // Stop processing additional receipt rules in the rule set.
      callback(null, {
        disposition: 'stop_rule_set',
      });
    }
  });

  // 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();  
    }  
};
```

S3-Aktion

Die S3-Aktion stellt die E-Mail einem Amazon S3 Bucket zu und benachrichtigt Sie optional über Amazon SNS. Diese Aktion umfasst die folgenden Optionen.

- **S3-Bucket**—Der Name des Amazon S3 Buckets, in dem die empfangenen E-Mails gespeichert werden sollen. Sie können einen neuen Amazon S3 Bucket auch beim Einrichten Ihrer Aktion erstellen, indem Sie **Erstellen eines S3-Buckets**. 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

Wenn Sie Ihre E-Mails in einem Amazon S3-Bucket speichern, beträgt die maximale E-Mail-Größe (einschließlich Header) 30 MB.

- **Präfix des Objektschlüssels** —Ein Schlüsselnamenpräfix zur Verwendung im Amazon S3 Bucket. Mit Schlüsselnamenpräfixen können Sie Ihren Amazon S3 Bucket in einer Ordnerstruktur organisieren. Wenn Sie beispielsweise `E-Mail` als Ihre Präfix für Objektschlüsselpräfix werden, Ihre E-Mails in Ihrem Amazon S3 Bucket in einem Ordner mit dem Namen `E-Mail` angezeigt.
- **KMS-Schlüssel** (wenn „Encrypt Message“ in der Amazon SES Konsole ausgewählt ist) —Der benutzerdefinierte Masterschlüssel, den Amazon SES verwenden soll, um Ihre E-Mails vor dem Speichern im Amazon S3-Bucket zu verschlüsseln. Sie können den Standardmasterschlüssel oder einen benutzerdefinierten Masterschlüssel, den Sie in AWS KMS erstellt haben, verwenden.

Note

Der Masterschlüssel, den Sie auswählen, muss sich in derselben AWS Region wie der Amazon SES S-Endpunkt befinden, den Sie zum Empfangen von E-Mails verwenden.

- Um den Standardmasterschlüssel zu verwenden, wählen Sie `aws/ses`. Wenn Sie die Empfangsregel in der Amazon SES Konsole einrichten. Wenn Sie die Amazon SES API verwenden, können Sie den Standardmasterschlüssel mit einem ARN in Form von `arn:aws:kms:REGION:AWSACCOUNTID:alias/aws/ses`. Wenn Ihre AWS Konto-ID beispielsweise `123456789012` lautet und Sie den Standardmasterschlüssel in der Region `USA West (Oregon)` verwenden möchten, lautet der ARN des Standardmasterschlüssels `arn:aws:kms:us-west-2:123456789012:alias/aws/ses`. Wenn Sie den Standard-Masterschlüssel verwenden, müssen Sie keine zusätzlichen Schritte durchführen, um Amazon SES die Berechtigung zur Verwendung des Schlüssels zu erteilen.
- Um einen benutzerdefinierten Masterschlüssel zu verwenden, den Sie in `AWS KMS` erstellt haben, geben Sie den ARN des Masterschlüssels an und stellen Sie sicher, dass Sie der Richtlinie Ihres Schlüssels eine Anweisung hinzufügen, um Amazon SES die Berechtigung zu seiner Verwendung zu erteilen. Weitere Informationen zum Erteilen von Berechtigungen finden Sie unter [Erteilen von Berechtigungen für Amazon SES für den E-Mail-Empfang](#) (p. 235).

Weitere Informationen zur Verwendung von `AWS KMS` mit Amazon SES, lesen Sie die [AWS Key Management Service Entwicklerhandbuch](#). Wenn Sie keinen Masterschlüssel in der Konsole oder der API angeben, werden Ihre E-Mail-Nachrichten von Amazon SES nicht verschlüsselt.

Important

Ihre E-Mail wird von Amazon SES mit dem Amazon S3-Verschlüsselungsclient verschlüsselt, bevor die E-Mail zur Speicherung an Amazon S3 übermittelt wird. Sie ist nicht mit der serverseitigen Verschlüsselung von Amazon S3 verschlüsselt. Das bedeutet, dass Sie die E-

Mails mit dem Amazon S3 Verschlüsselungscient entschlüsseln müssen, nachdem Sie sie von Amazon S3 abgerufen haben, da der Service keinen Zugriff auf Ihre AWS KMS Schlüssel für die Entschlüsselung. Dieser Verschlüsselungs-Client ist in [AWS SDK for Java](#) und [AWS SDK for Ruby](#) verfügbar. Weitere Informationen zur clientseitigen Verschlüsselung mit AWS KMS Master-Schlüssel finden Sie im [Amazon Simple Storage Service – Entwicklerhandbuch](#).

- **SNS-Thema-Programm** Der Name oder ARN des Amazon SNS -Themas, das benachrichtigt werden soll, wenn eine E-Mail im Amazon S3 Bucket gespeichert werden soll. Ein ARN eines Amazon SNS -Themas ist beispielsweise: `arn:sns:us-west-2:123456789012:MyTopic`. Sie können ein Amazon SNS Topic auch beim Einrichten Ihrer Aktion erstellen, indem Sie Erstellen eines SNS-Themas. Weitere Informationen zu Amazon SNS -Themen finden Sie im [Amazon Simple Notification Service-Entwicklerhandbuch](#).

Note

Das Amazon SNS -Thema, das Sie auswählen, muss sich in derselben AWS Region wie der Amazon SES S-Endpunkt befinden, den Sie zum Empfangen von E-Mails verwenden.

SNS-Aktion

Die SNS veröffentlicht die E-Mail mit einer Amazon SNS Benachrichtigung. Die Benachrichtigung enthält die vollständigen E-Mail-Inhalte. Diese Aktion umfasst die folgenden Optionen.

- **SNS-Thema-Programm** Der Name oder ARN des Amazon SNS Topics, für das die E-Mails veröffentlicht werden sollen. Die Amazon SNS Benachrichtigungen enthalten eine unformatierte, unveränderte Kopie der E-Mail, die in der Regel das Format Multipurpose Internet Mail Extensions (MIME) hat. 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 ARN eines Amazon SNS -Themas ist beispielsweise: `arn:sns:us-west-2:123456789012:MyTopic`. Sie können ein Amazon SNS Topic auch beim Einrichten Ihrer Aktion erstellen, indem Sie Erstellen eines SNS-Themas. Weitere Informationen zu Amazon SNS -Themen finden Sie im [Amazon Simple Notification Service-Entwicklerhandbuch](#).

Note

Das Amazon SNS -Thema, das Sie auswählen, muss sich in derselben AWS Region wie der Amazon SES S-Endpunkt befinden, den Sie zum Empfangen von E-Mails verwenden.

- **Kodierung** —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 Kodierungsformat kodiert wurde. Base64 bewahrt alle Sonderzeichen. Weitere Informationen zu UTF-8 und Base64 finden Sie in [RFC 3629](#) bzw. [RFC 4648](#).

Stop-Aktion

Die Aktion beendet die Auswertung des Empfangsregelsatzes und benachrichtigt Sie optional über Amazon SNS. Diese Aktion umfasst die folgenden Optionen.

- **SNS-Thema-Programm** Der Name oder ARN des Amazon SNS Topics, das benachrichtigt werden soll, wenn die Stop-Aktion ausgeführt wird. Ein ARN eines Amazon SNS -Themas ist beispielsweise: `arn:sns:us-west-2:123456789012:MyTopic`. Sie können ein Amazon SNS Topic auch beim Einrichten Ihrer Aktion erstellen, indem Sie Erstellen eines SNS-Themas. Weitere Informationen zu Amazon SNS -Themen finden Sie im [Amazon Simple Notification Service-Entwicklerhandbuch](#).

Das Amazon SNS -Thema, das Sie auswählen, muss sich in derselben AWS Region wie der Amazon SES S-Endpoint befinden, den Sie zum Empfangen von E-Mails verwenden.

Die WorkMail-Aktion kann in Amazon WorkMail integriert werden. Wenn Amazon WorkMail die gesamte E-Mail-Verarbeitung ausführt, verwenden Sie diese Aktion in der Regel nicht direkt, da Amazon WorkMail die Einrichtung übernimmt. Diese Aktion umfasst die folgenden Optionen.

- Organisation ARN —Der ARN der Amazon WorkMail-Organisation.
ARNs der Amazon WorkMail Organisation liegen im Format
vorarn:aws:workmail:region:account_ID:organization/organization_ID, dabei gilt:
 - regiondie Region ist, in der Sie Amazon SES und Amazon WorkMail verwenden. (Sie müssen sie in der gleichen Region verwenden.) Beispiel: us-west-2
 - account_IDist die AWS Konto-ID. Sie finden Ihre AWS Konto-ID auf der Seite [Konto](#)Seite der AWS Management Console (AWS Management Console)
 - organization_IDeine eindeutige ID ist, die Amazon WorkMail generiert, wenn Sie eine Organisation erstellen. Sie finden die Organisations-ID in der Amazon WorkMail Konsole auf der Seite „Organization Settings“ Ihres Unternehmens.

[illegible]

- SNS-Thema-ProgrammDer Name oder ARN des Amazon SNS -Themas, das benachrichtigt werden soll, wenn die Amazon WorkMail Aktion ausgeführt wird. Ein ARN eines Amazon SNS -Themas ist beispielsweise:arn:sns:us-west-2:123456789012:MyTopic. Sie können ein Amazon SNS Topic auch beim Einrichten Ihrer Aktion erstellen, indem SieErstellen eines SNS-Themas. Weitere Informationen zu Amazon SNS -Themen finden Sie im.[Amazon Simple Notification Service-Entwicklerhandbuch](#).

Das Amazon SNS -Thema, das Sie auswählen, muss sich in derselben AWS Region wie der Amazon SES S-Endpoint befinden, den Sie zum Empfangen von E-Mails verwenden.

Nachdem Sie Ihren Empfangsregelsatz sowie die Empfangsregeln und IP-Adressenfilter erstellt haben, können Sie mithilfe der Amazon SES Konsole oder der API andere Operationen bearbeiten, löschen oder ausführen. Sie können außerdem die Amazon SNS Benachrichtigungen, die Sie erhalten, prüfen und die Fehlermetriken in Amazon CloudWatch anzeigen.

- [Verwalten von Wareneingangsregelsätzen für Amazon SES E-Mail-Empfang \(p. 253\)](#)
- [Verwalten von Zahlungsregeln für Amazon SES E-Mail-Empfang \(p. 255\)](#)
- [Verwalten von IP-Adressfiltern für Amazon SES E-Mail-Empfang \(p. 258\)](#)
- [Anzeigen von Metriken für Amazon SES E-Mail-Empfang \(p. 258\)](#)
- [Verwenden von Benachrichtigungen für Amazon SES E-Mail-Empfang \(p. 259\)](#)

Verwalten von Wareneingangsregelsätzen für Amazon SES E-Mail-Empfang

Nach dem Erstellen eines Empfangsregelsatzes, wie in [Erstellen eines Empfangsregel](#) (p. 238) beschrieben, können Sie ihn nach Bedarf aktualisieren. Obwohl das Bearbeiten eines Empfangsregelsatzes in der Regel durch Ändern einzelner Empfangsregeln besteht, wie in [Verwalten von Empfangsregeln](#) (p. 255) beschrieben, können Sie Empfangsregelsätze auch löschen, aktivieren, deaktivieren und kopieren. Außerdem können Sie die Empfangsregeln in einem Empfangsregelsatz neu anordnen. Diese Operationen in den folgenden Abschnitten erläutert.

Themen in diesem Abschnitt:

- [Löschen eines Empfangsregelsatzes](#) (p. 253)
- [Aktivieren und Deaktivieren eines Empfangsregelsatzes](#) (p. 253)
- [Kopieren eines Empfangsregelsatzes](#) (p. 254)
- [Neuanordnen von Empfangsregeln](#) (p. 255)

Löschen eines Empfangsregelsatzes

Sie können die Amazon SES Konsole oder die `DeleteReceiptRuleSet`-API zum Löschen eines Empfangsregelsatzes.

Note

Ein Empfangsregelsatz, der derzeit aktiv ist, kann nicht gelöscht werden.

So löschen Sie einen Empfangsregelsatz (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Klicken Sie in der Liste Inactive Rule Sets auf den Empfangsregelsatz, den Sie löschen möchten.
4. Wählen Sie im Menü Actions die Option Delete aus und bestätigen Sie anschließend, dass Sie den Empfangsregelsatz löschen möchten.

Weitere Informationen zur Verwendung der `DeleteReceiptRuleSet`-API zum Löschen eines Empfangsregelsatzes finden Sie weitere Informationen unter der [Amazon Simple Email Service API-Referenz](#) [Referenz](#) für.

Aktivieren und Deaktivieren eines Empfangsregelsatzes

Für jeden Empfangsregelsatz sind zwei Zustände möglich: aktiviert oder deaktiviert. Es kann jeweils nur ein Empfangsregelsatz aktiv sein. Deaktivierte Empfangsregelsätze können in Fällen sinnvoll sein, in denen Sie Änderungen an Ihrem aktiven Empfangsregelsatz vornehmen möchten, diese Änderungen aber erst aktiv werden sollen, wenn Sie sicher sind, dass Ihre Updates korrekt sind. In diesem Fall können Sie den aktiven Empfangsregelsatz kopieren und die Änderungen am kopierten, deaktivieren Empfangsregelsatz vornehmen. Nachdem Sie die Änderungen überprüft haben, können Sie den kopierten Empfangsregelsatz aktivieren. Wenn Sie einen Empfangsregelsatz aktivieren, werden alle anderen Empfangsregelsätze automatisch deaktiviert.

Note

Um den E-Mail-Empfang über Amazon SES ganz einzustellen, deaktivieren Sie alle Empfangsregelsätze.

Sie können die Amazon SES Konsole oder die `SetActiveReceiptRuleSet`-API, um zu kontrollieren, welcher Empfangsregelsatz aktiv ist.

So aktivieren Sie einen deaktivierten Empfangsregelsatz (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Klicken Sie in der Liste Inactive Rule Sets auf den Empfangsregelsatz, den Sie aktivieren möchten.
4. Wählen Sie Set as Active Rule Set aus.

So deaktivieren Sie einen aktivierten Empfangsregelsatz (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Wählen Sie unter Active Rule Set die Option Disable Active Rule Set aus und bestätigen Sie anschließend, dass Sie den Empfangsregelsatz deaktivieren möchten.

Weitere Informationen zur Verwendung der `SetActiveReceiptRuleSet`-API zum Aktivieren oder Deaktivieren eines Regelsatzes finden Sie weitere Informationen unter der [Amazon Simple Email Service API-Referenz Referenz](#) für.

Kopieren eines Empfangsregelsatzes

Sie können die Amazon SES Konsole oder die `CloneReceiptRuleSet`-API zum Kopieren eines Empfangsregelsatzes. Wenn Sie die Amazon SES Konsole verwenden, weicht das Verfahren geringfügig ab, je nachdem, ob der Empfangsregelsatz, den Sie kopieren möchten, aktiv oder deaktiviert ist.

So kopieren Sie einen aktivierten Empfangsregelsatz (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Wählen Sie im Inhaltsbereich Copy Active Rule Set aus.
4. Geben Sie im Dialogfeld Copy Rule Set den Namen ein, den Sie dem kopierten Empfangsregelsatz zuweisen möchten.
5. Wählen Sie Copy Rule Set aus. Der kopierte Empfangsregelsatz wird in der Liste Inactive Rule Sets angezeigt.

So kopieren Sie einen deaktivierten Empfangsregelsatz (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Klicken Sie in der Liste Inactive Rule Sets auf den Empfangsregelsatz, den Sie kopieren möchten.
4. Wählen Sie im Menü Actions die Option Copy aus.
5. Geben Sie im Dialogfeld Copy Rule Set den Namen ein, den Sie dem kopierten Empfangsregelsatz zuweisen möchten.
6. Wählen Sie Copy Rule Set aus. Der kopierte Empfangsregelsatz wird in der Liste Inactive Rule Sets angezeigt.

Weitere Informationen zur Verwendung des `CloneReceiptRuleSet`-API zum Kopieren eines Empfangsregelsatzes finden Sie weitere Informationen unter der [Amazon Simple Email Service API-Referenz](#) für.

Neuanordnen von Empfangsregeln

Sie können die Amazon SES Konsole oder die `ReorderReceiptRuleSet`-API verwenden, um Empfangsregeln in einem Empfangsregelsatz neu anzuordnen. Wenn Sie die Amazon SES Konsole verwenden, weicht das Verfahren geringfügig ab, je nachdem, ob der Empfangsregelsatz aktiv oder deaktiviert ist.

So ordnen Sie die Empfangsregeln im aktiven Empfangsregelsatz neu an (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Wählen Sie im Inhaltsbereich View Active Rule Set aus.
4. Klicken Sie auf Reorder Rules.
5. Ordnen Sie die Empfangsregeln mit den Pfeilen nach oben und nach unten neben den entsprechenden Namen neu an und wählen Sie Save Order aus.

So ordnen Sie die Empfangsregeln in einem deaktivierten Empfangsregelsatz neu an (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Wählen Sie in der Liste Inactive Rule Sets den Empfangsregelsatz aus.
4. Klicken Sie auf Reorder Rules.
5. Ordnen Sie die Empfangsregeln mit den Pfeilen nach oben und nach unten neben den entsprechenden Namen neu an und wählen Sie Save Order aus.

Weitere Informationen zur Verwendung des `ReorderReceiptRuleSet`-API zum Neuanordnen von Empfangsregeln in einem Empfangsregelsatz finden Sie weitere Informationen unter der [Amazon Simple Email Service API-Referenz](#) für.

Verwalten von Zahlungsregeln für Amazon SES E-Mail-Empfang

Zusätzlich zum Erstellen von Empfangsregeln wie in [Erstellen von Empfangsregeln \(p. 239\)](#) beschrieben, können Sie eine Empfangsregel in dem entsprechenden Empfangsregelsatz bearbeiten, löschen, aktivieren, deaktivieren, kopieren und ihre Position festlegen, wie in den folgenden Abschnitten beschrieben.

Note

Die Anweisungen in diesem Abschnitt setzen voraus, dass sich die Empfangsregel im aktiven Empfangsregelsatz befindet. Zum Bearbeiten der Empfangsregeln eines deaktivierten Empfangsregelsatzes wählen Sie einen entsprechenden Satz in der Liste Inactive Rule Sets aus. Die darauffolgenden Schritte zum Bearbeiten von Empfangsregeln sind die gleichen wie für den aktiven Empfangsregelsatz.

Themen in diesem Abschnitt:

- [Bearbeiten einer Empfangsregel \(p. 256\)](#)
- [Löschen einer Empfangsregel \(p. 256\)](#)
- [Aktivieren und Deaktivieren einer Empfangsregel \(p. 256\)](#)
- [Kopieren einer Empfangsregel \(p. 257\)](#)
- [So legen Sie die Position einer Empfangsregel fest \(p. 257\)](#)

Bearbeiten einer Empfangsregel

Sie können die Amazon SES -Konsole oder die Amazon SES -API verwenden, um eine Empfangsregel zu bearbeiten. Amazon SES-Konsole ist einfacher, die Amazon SES Konsole zu verwenden.

So bearbeiten Sie eine Empfangsregel (Konsole)

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Klicken Sie im Inhaltsbereich auf View Active Rule Set oder wählen Sie einen Empfangsregelsatz in der Liste Inactive Rule Sets aus.
4. Klicken Sie im Detailbereich auf die Empfangsregel, die Sie bearbeiten möchten.
5. Bearbeiten Sie die Richtlinie im Bereich Edit Rule und wählen Sie anschließend Save Rule aus.

Wenn Sie stattdessen die Amazon SES API verwenden möchten, verwenden Sie dieDescribeReceiptRule-API abrufen, mithilfe eines Texteditors bearbeiten und anschließend denUpdateReceiptRule-API verwenden, um die vorherige Version der Regel zu überschreiben. Weitere Informationen finden Sie im [Amazon Simple Email Service API-Referenz Referenz für](#).

Löschen einer Empfangsregel

Sie können die Amazon SES Konsole oder dieDeleteReceiptRule-API zum Löschen einer Empfangsregel.

So löschen Sie eine Empfangsregel (Konsole)

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Klicken Sie im Inhaltsbereich auf View Active Rule Set oder wählen Sie einen Empfangsregelsatz in der Liste Inactive Rule Sets aus.
4. Klicken Sie im Detailbereich auf die gewünschte Empfangsregel.
5. Wählen Sie im Menü Actions die Option Delete aus und bestätigen Sie anschließend, dass Sie die Empfangsregel löschen möchten.

Weitere Informationen zur Verwendung desDeleteReceiptRule-API zum Löschen einer Regel finden Sie unter[Amazon Simple Email Service API-Referenz Referenz für](#).

Aktivieren und Deaktivieren einer Empfangsregel

Sie können die Amazon SES -Konsole oder die Amazon SES -API verwenden, um eine Empfangsregel zu aktivieren oder zu deaktivieren. Amazon SES-Konsole ist einfacher, die Amazon SES Konsole zu verwenden.

So aktivieren oder deaktivieren Sie eine Empfangsregel (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Klicken Sie im Inhaltsbereich auf View Active Rule Set oder wählen Sie einen Empfangsregelsatz in der Liste Inactive Rule Sets aus.
4. Klicken Sie im Detailbereich auf die Empfangsregel, die Sie bearbeiten möchten.
5. Wählen Sie im Bereich Edit Rule die Option Enabled aus oder heben Sie die Auswahl auf und klicken Sie anschließend auf Save Rule.

Wenn Sie stattdessen die Amazon SES API verwenden möchten, können Sie die `DescribeReceiptRule`-API, um die Zahlungsregel abzurufen, verwenden Sie einen Texteditor, um die `Enabled`, und verwenden Sie dann das `UpdateReceiptRule`-API verwenden, um die vorherige Version der Empfangsregel zu überschreiben. Weitere Informationen finden Sie im [Amazon Simple Email Service API-Referenz](#) für.

Kopieren einer Empfangsregel

Sie können die Amazon SES -Konsole oder die Amazon SES -API verwenden, um eine Empfangsregel zu kopieren. Amazon SES-Konsole ist einfacher, die Amazon SES Konsole zu verwenden.

So kopieren Sie eine Empfangsregel (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Klicken Sie im Inhaltsbereich auf View Active Rule Set oder wählen Sie einen Empfangsregelsatz in der Liste Inactive Rule Sets aus.
4. Klicken Sie im Detailbereich auf die gewünschte Empfangsregel.
5. Wählen Sie im Menü Actions die Option Copy Rule aus.
6. Geben Sie im Dialogfeld Copy Rule einen neuen Namen für die Empfangsregel ein und wählen Sie den gewünschten Empfangsregelsatz aus. Die neue Empfangsregel wird am Anfang des Empfangsregelsatzes eingefügt und anfänglich deaktiviert.

Wenn Sie stattdessen die Amazon SES API verwenden möchten, können Sie die `DescribeReceiptRule`-API abrufen, den Namen der Empfangsregel und ggf. den Empfangsregelsatz mit einem Texteditor bearbeiten und diese Empfangsregel der `CreateReceiptRule`-API. Weitere Informationen finden Sie im [Amazon Simple Email Service API-Referenz](#) für.

So legen Sie die Position einer Empfangsregel fest

Sie können die Amazon SES Konsole oder die `SetReceiptRulePosition`-API, um die Position einer Empfangsregel in einem Empfangsregelsatz zu ändern.

So legen Sie die Position einer Empfangsregel fest (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option Rule Sets aus.
3. Klicken Sie im Inhaltsbereich auf View Active Rule Set oder wählen Sie einen Empfangsregelsatz in der Liste Inactive Rule Sets aus.
4. Wählen Sie im Inhaltsbereich Reorder Rules aus.

5. Ordnen Sie die Empfangsregeln mit den Pfeilen nach oben und nach unten neben den entsprechenden Namen neu an und wählen Sie Save Order aus.

Weitere Informationen zur Verwendung des `SetReceiptRulePosition`-API, um die Position einer Empfangsregel in einem Empfangsregelsatz zu ändern, finden Sie unter [Amazon Simple Email Service API-Referenz](#) für.

Verwalten von IP-Adressfiltern für Amazon SES E-Mail-Empfang

Zusätzlich zum Erstellen von IP-Adressenfiltern, wie in [Erstellen von IP-Adressenfilter \(p. 238\)](#) beschrieben, können Sie Filter anzeigen und löschen, wie in den folgenden Abschnitten erläutert.

Anzeigen von IP-Adressenfiltern

Sie können die Amazon SES Konsole oder die `ListReceiptFilters`-API, um eine Liste Ihrer IP-Adressenfilter aufzurufen.

So zeigen Sie Ihre IP-Adressenfilter an (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option IP Address Filters aus. Es wird eine Liste mit Ihren IP-Adressenfiltern angezeigt.

Weitere Informationen zur Verwendung des `ListReceiptFilters`-API, um eine Liste Ihrer IP-Adressenfilter aufzurufen, finden Sie weitere Informationen unter der [Amazon Simple Email Service API-Referenz](#) für.

das Löschen eines IP-Adressfilters

Sie können die Amazon SES Konsole oder die `DeleteReceiptFilter`-API zum Löschen eines IP-Adressfilters.

So löschen Sie einen IP-Adressenfilter (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich unter Email Receiving die Option IP Address Filters aus.
3. Wählen Sie den IP-Adressenfilter im Detailbereich aus.
4. Klicken Sie auf Delete und bestätigen Sie, dass Sie den IP-Adressenfilter löschen möchten.

Weitere Informationen zur Verwendung des `DeleteReceiptFilter`-API zum Löschen eines IP-Adressfilters finden Sie weitere Informationen unter der [Amazon Simple Email Service API-Referenz](#) für.

Anzeigen von Metriken für Amazon SES E-Mail-Empfang

Sie können Amazon CloudWatch (CloudWatch) verwenden, um Fehlermetriken für Ihre Empfangsregeln anzuzeigen. Sie finden die Metriken unter SES/Rule Metrics.

Es gibt zwei Arten von Fehlermetriken:

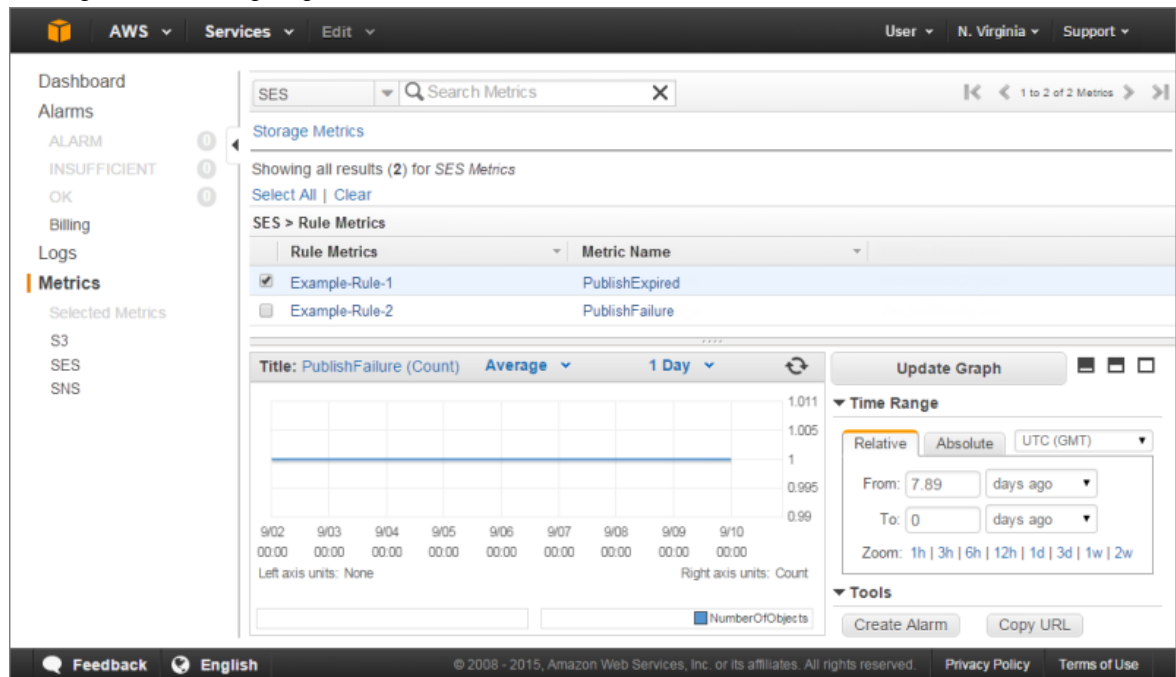
- **PublishFailure**— In Amazon SES ist ein Fehler aufgetreten bei dem Versuch, die Aktionen auszuführen, die Sie konfiguriert haben.
- **PublishExpired**— In Amazon SES ist ein Fehler aufgetreten bei dem Versuch, die Aktionen auszuführen, die Sie konfiguriert haben, und Amazon SES versucht nicht mehr die E-Mail zuzustellen. Dieser Fehler kann dauerhaft oder vorübergehend sein. Amazon SES wiederholt die Aktion nicht mehr, da sie innerhalb von vier Stunden nicht erfolgreich ausgeführt wurde.

Diese 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 Empfangsregel konfiguriert war.

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.

Die folgende Abbildung zeigt die Metriken in der CloudWatch Konsole.



Verwenden von Benachrichtigungen für Amazon SES E-Mail-Empfang

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:

- **Benachrichtigungen, die von SNS-Aktionen gesendet werden**— Wenn Sie eine [SNS \(p. 251\)](#)-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.

- Benachrichtigungen, die von anderen Aktionstypen gesendet werden— Wenn Sie einen anderen Aktionstyp hinzufügen (einschließlich [Unzustellbarkeit](#) (p. 242), [Lambda](#) (p. 242), [Stopp-Regelsatz](#) (p. 251), oder [WorkMail](#) (p. 252)-Aktionen) zu einer Zahlungsregel hinzufügen, können Sie optional ein Amazon 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 dieser Benachrichtigungen beschrieben und es wird ein Beispiel für jeden Benachrichtigungstyp angegeben.

Themen in diesem Abschnitt:

- [Inhalt der Benachrichtigungen für den Erhalt von Amazon SES E-Mails](#) (p. 260)
- [Beispiele für Benachrichtigungen für Amazon SES E-Mail-Empfang](#) (p. 266)

Inhalt der Benachrichtigungen für den Erhalt von Amazon SES E-Mails

Alle Benachrichtigungen für den E-Mail-Empfang werden in Amazon SNS (Simple Notification Service) -Themen im JavaScript Object Notation (JSON) -Format veröffentlicht.

JSON-Objekt der obersten Ebene

Das JSON-Objekt der obersten Ebene enthält die folgenden Felder.

Feldname	Beschreibung
<code>notificationType</code>	Der Benachrichtigungstyp. Für diese Art der Benachrichtigung lautet der Wert immer <code>Received</code> .
receipt (p. 260)	Ein Objekt, das Informationen über die E-Mail-Zustellung enthält.
mail (p. 265)	Ein Objekt, das Informationen zur E-Mail enthält, die der Benachrichtigung zugeordnet ist.
<code>content</code>	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. 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.

Empfangs-Objekt

Das `receipt`-Objekt enthält folgende Felder.

Feldname	Beschreibung
action (p. 262)	Ein Objekt, das Informationen über die Aktion kapselt, die ausgeführt wurde. Eine Liste möglicher Werte finden Sie unter action -Objekt (p. 262).
dkimVerdict (p. 263)	Ein Objekt das, angibt, ob die DomainKeys Identified Mail (DKIM)-Prüfung bestanden wurde. Eine Liste möglicher Werte finden Sie unter dkimVerdict Object (p. 263).
<code>dmARCPolicy</code>	Gibt die DMARC-Einstellungen (Domain-based 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: • <code>none</code>: Der Eigentümer der sendenden Domäne verlangt, dass bei Nachrichten, bei denen die DMARC-Authentifizierung fehlschlägt, keine bestimmte Aktion ausgeführt wird. • <code>quarantine</code>: Der Eigentümer der sendenden Domäne verlangt, dass Nachrichten, für die die DMARC-Authentifizierung fehlschlägt, von Receivern als verdächtig eingestuft werden. • <code>reject</code>: Der Eigentümer der sendenden Domäne verlangt, dass Nachrichten, für die die DMARC-Authentifizierung fehlschlägt, abgelehnt werden.
dmARCVerdict (p. 263)	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 (p. 263).
<code>processingTimeMillis</code>	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.
<code>recipients</code>	Eine Liste von Empfängern (speziell die Envelope-RCPT TO-Adressen), die der aktiven Empfangsregel (p. 239) entsprachen. Die hier aufgelisteten Adressen können sich von den Adressen unterscheiden, die von dem Feld <code>destination</code> im the section called "Mail-Objekt" (p. 265) aufgelistet werden.
spamVerdict (p. 264)	Ein Objekt, das angibt, ob es sich bei der Nachricht um Spam handelt. Eine Liste möglicher Werte finden Sie unter SpamVerdict Object (p. 264).
spfVerdict (p. 264)	Ein Objekt das angibt, ob die Sender Policy Framework (SPF)-Prüfung bestanden wurde. Eine

Feldname	Beschreibung
	Liste möglicher Werte finden Sie unter spfVerdict Object (p. 264).
timestamp	Eine Zeichenfolge, die das Datum und die Uhrzeit angibt, zu der die Aktion ausgelöst wurde, in ISO 8601 .
virusVerdict (p. 264)	Ein Objekt, das angibt, ob die Nachricht einen Virus enthält. Eine Liste möglicher Werte finden Sie unter VirusVerdict Object (p. 264).

[action](#) -Objekt

Das [action](#)-Objekt enthält folgende Felder.

Feldname	Beschreibung
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-Ressourcennamen (ARN) des Amazon SNS - Themas, in der die Benachrichtigung veröffentlicht wurde.
bucketName	Eine Zeichenfolge mit dem Namen des Amazon S3 Buckets, in dem die Nachricht 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 <code>messageId</code> im the section called "Mail-Objekt" (p. 265). 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.

Feldname	Beschreibung
<code>functionArn</code>	Eine Zeichenfolge mit dem ARN der Lambda - Funktion, die ausgelöst wurde. Diese ist nur für den Lambda-Aktionstyp vorhanden.
<code>invocationType</code>	Eine Zeichenfolge mit dem Aufruftyp der Lambda - Funktion. Mögliche Werte sind <code>RequestResponse</code> und <code>Event</code> . Diese ist nur für den Lambda-Aktionstyp vorhanden.
<code>organizationArn</code>	Eine Zeichenfolge mit dem ARN der Amazon WorkMail-Organisation. Diese ist nur für den WorkMail-Aktionstyp vorhanden.

dkimVerdict Object

Das `dkimVerdict`-Objekt enthält folgende Felder.

Feldname	Beschreibung
<code>status</code>	Eine Zeichenfolge mit dem DKIM-Prüfungsergebnis. Die möglichen Werte sind: • <code>PASS</code>: Die Nachricht hat die DKIM-Authentifizierung bestanden. • <code>FAIL</code>: Die Nachricht hat die DKIM-Authentifizierung nicht bestanden. • <code>GRAY</code>: Die Nachricht ist nicht mit einer DKIM-Signatur versehen. • <code>PROCESSING_FAILED</code>: 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	Beschreibung
<code>status</code>	Eine Zeichenfolge mit dem DMARC-Prüfungsergebnis. Die möglichen Werte sind: • <code>PASS</code>: Die Nachricht hat die DMARC-Authentifizierung bestanden. • <code>FAIL</code>: Die DMARC-Authentifizierung für die Nachricht ist fehlgeschlagen. • <code>GRAY</code>: Die DMARC-Authentifizierung für die Nachricht ist fehlgeschlagen und die sendende Domäne verfügt nicht über eine DMARC-Richtlinie oder verwendet die <code>p=none</code>-Richtlinie.

Feldname	Beschreibung
	• 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	Beschreibung
<code>status</code>	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. • PROCESSING_FAILED: Amazon SES konnte die E-Mail nicht scannen. Bei der E-Mail handelt es sich beispielsweise nicht um eine gültige MIME-Nachricht.

spfVerdict Object

Das `spfVerdict`-Objekt enthält folgende Felder.

Feldname	Beschreibung
<code>status</code>	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: Es gibt keine SPF-Richtlinie für die Domäne, die im MAIL FROM-Befehl verwendet wurde. • 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	Beschreibung
<code>status</code>	Eine Zeichenfolge mit dem Ergebnis der Virusprüfung. Die möglichen Werte sind: • <code>PASS</code>: Die Nachricht enthält keine Viren. • <code>FAIL</code>: Die Nachricht enthält einen Virus. • <code>GRAY</code>: Amazon SES hat die E-Mail geprüft, konnte aber nicht mit Sicherheit ermitteln, ob sie einen Virus enthält. • <code>PROCESSING_FAILED</code>: 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	Beschreibung
<code>destination</code>	Eine vollständige Liste aller Empfängeradressen (einschließlich To: – und CC: -Empfänger) aus den MIME-Headern der eingehenden E-Mail.
<code>messageId</code>	Eine Zeichenfolge mit der eindeutigen ID, die der E-Mail von Amazon SES zugewiesen wurde. Wenn die E-Mail Amazon S3 zugestellt wurde, ist die Mitteilungs-ID gleichzeitig der Amazon S3-Objektschlüssel, mit dem die Nachricht in Ihren Amazon S3-Bucket geschrieben wurde.
<code>source</code>	Eine Zeichenfolge mit der E-Mail-Adresse (speziell der Envelope-MAIL FROM-Adresse), von der die E-Mail gesendet wurde.
<code>timestamp</code>	Eine Zeichenfolge mit dem Zeitpunkt, zu dem die E-Mail empfangen wurde, im ISO8601-Format.
<code>headers</code>	Eine Liste der Amazon SES Header und Ihren benutzerdefinierten Header. Jeder Header in der Liste verfügt über die Felder <code>name</code> und <code>value</code> .
<code>commonHeaders</code> (p. 266)	Eine Liste der Header für alle E-Mails. Jeder Header in der Liste besteht aus einem Namen und einem Wert.
<code>headersTruncated</code>	Gibt an, ob die Header in der Benachrichtigung abgeschnitten wurden. Dies passiert, wenn die Header größer als 10 KB sind. Mögliche Werte sind <code>true</code> und <code>false</code> .

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	Beschreibung
<code>messageId</code>	Die ID der ursprünglichen Nachricht.
<code>date</code>	Das Datum und die Uhrzeit, als Amazon SES die Nachricht erhalten hat.
<code>to</code>	Die Werte im "To" (An)-Header der E-Mail.
<code>cc</code>	Die Werte im "CC"-Header der E-Mail.
<code>bcc</code>	Die Werte im "BCC"-Header der E-Mail.
<code>from</code>	Die Werte im "From" (Von)-Header der E-Mail.
<code>sender</code>	Die Werte im "Sender" (Sender)-Header der E-Mail.
<code>returnPath</code>	Die Werte im "Return-Path" (Rücksendepfad)-Header der E-Mail.
<code>reply-to</code>	Die Werte im "Reply-To" (Antworten an)-Header der E-Mail.
<code>subject</code>	Der Wert des "Subject" (Betreff)-Headers für die E-Mail.

Beispiele für Benachrichtigungen für Amazon SES E-Mail-Empfang

Dieser Abschnitt enthält Beispiele für die folgenden Arten von Benachrichtigungen:

- [Eine Benachrichtigung, die als Ergebnis einer SNS-Aktion gesendet wird. \(p. 266\)](#)
- [Eine Benachrichtigung, die aufgrund einer anderen Art der Aktion gesendet wird \(p. 268\) \(eine Warnungsbenachrichtigung\).](#)

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 MIME-Format (Multipurpose Internet Mail Extensions) 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-BEC9-87CBCE2211C9@example.com",
    "messageId":"d6iitobk75ur44p8kdnp7g2n800",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"Return-Path",

"value":"<0000014fbc1c09cf-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
d6iitobk75ur44p8kdnp7g2n800 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=ug7nbtff4gccmlpwj322ax3p6ow6yfsug; 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=p4ukUDSFqhqiuub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF
hlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
4hHstlXPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g="
      },
      {
        "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\nts=ug7nbt4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;\r\n\th=From:To:Subject:MIME-Version:Content-Transfer-Encoding:Date:Message-ID:Feedback-ID;\r\n\tbh=DWr3IOMYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;\r\n\tb=p4ukUDSFqhqiub+zPRODW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF\r\n\tlX30v7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX\r\n\t4hHst1XPyX5wmgdHIhmUuh8oZKpVqG16bHGzzf7g=\r\n\tFrom: sender@example.com\r\n\tTo: recipient@example.com\r\n\tSubject: Example subject\r\n\tMIME-Version: 1.0\r\n\tContent-Type: text/plain; charset=UTF-8\r\n\tContent-Transfer-Encoding: 7bit\r\n\tDate: Fri, 11 Sep 2015 20:32:32 +0000\r\n\tMessage-ID: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>\r\n\tX-SES-Outgoing: 2015.09.11-54.240.9.183\r\n\tFeedback-ID: 1.us-east-1.Krv2FKpFdWV+KUYw3Qd6wcpPJ4Sv/pOPpEPShn2u2o4=:AmazonSES\r\n\r\n\tExample 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": "0000014fbelc09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
  "messageId": "d6iitobk75ur44p8kdnp7g2n800",
  "destination": [
    "recipient@example.com"
  ],
  "headersTruncated": false,
  "headers": [
    {
      "name": "Return-Path",
      "value": "<0000014fbelc09cf-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 d6iitobk75ur44p8kdnp7g2n800 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=ug7nbt4gccmlpwj322ax3p6ow6yfsug; 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+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJFh1X3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g="
    },
    {
      "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":
    "0000014fbelc09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-0000000@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"
}
}
```

Verwenden von Amazon SES Konfigurationssätzen

Konfigurationssätze sind Gruppen von Regeln, die Sie auf die E-Mails anwenden können, die Sie mit Amazon SES versenden. Sie wenden einen Konfigurationssatz auf eine E-Mail an, indem Sie einen Verweis auf den Konfigurationssatz in den Kopfzeilen der E-Mail einfügen. Wenn Sie einen Konfigurationssatz auf eine E-Mail anwenden, werden alle Regeln dieses Konfigurationssatzes auf die E-Mail angewendet. Weitere Informationen zum Festlegen von Konfigurationssätzen in Ihren E-Mails finden Sie unter [Festlegen eines Konfigurationssatzes für das Senden von E-Mail](#) (p. 279).

Mit Hilfe von Konfigurationssätzen können Sie die folgenden Arten von Regeln auf Ihre E-Mails anwenden:

- **Ereignisveröffentlichung**— Amazon SES kann die Anzahl der Sende-, Zustell-, Öffnungs-, Klick-, Unzustellbaren und Beschwerdeereignisse für jede von Ihnen gesendete E-Mail verfolgen. Sie können die Ereignisveröffentlichung verwenden, um Informationen über diese Ereignisse an andere AWS - Services zu senden. Beispielsweise können Sie Ihre E-Mail-Metriken an ein Amazon Kinesis Data Firehose hose-Ziel senden und diese dann mithilfe von Amazon Kinesis Data Analytics analysieren. Alternativ können Sie Unzustellbare 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 mieten, können Sie Gruppen dieser Adressen erstellen, die als IP-Pools aus. Diese dedizierten IP-Pools können Sie dann mit Konfigurationssätzen verknüpfen. Ein häufiger Anwendungsfall ist es, einen Pool von dedizierten IP-Adressen für den Versand von Marketingkommunikation und einen weiteren für den Versand von transaktionalen E-Mails zu erstellen. Ihre Absender-Reputation für transaktionale E-Mails wird dann von der für Ihre Marketing-E-Mails getrennt.

Konfigurationssätze können eine, beide oder keine dieser Arten von Regeln enthalten.

Weitere Informationen zur Verwaltung von Konfigurationssätzen und den dazugehörigen Komponenten finden Sie in den folgenden Abschnitten:

- [Verwalten von Konfigurationssätzen in Amazon SES](#) (p. 271)
- [Verwalten von Veranstaltungszielen in Amazon SES](#) (p. 277)
- [Verwalten von dedizierten IP-](#) (p. 278)

Verwalten von Konfigurationssätzen in Amazon SES

Dieser Abschnitt enthält Verfahren für das Erstellen von Konfigurationssätzen, das Anzeigen einer Liste mit Ihren vorhandenen Konfigurationssätzen, das Anzeigen von Details einzelner Konfigurationssätze und das Löschen von Konfigurationssätzen.

Erstellen eines Konfigurationssatzes

Sie können die Amazon SES Konsole oder die `CreateConfigurationSet`-API, um neue Konfigurationssätze zu erstellen.

So erstellen Sie einen Konfigurationssatz mithilfe der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich Configuration Sets aus.
3. Wählen Sie Create Configuration Set aus.
4. Geben Sie unter Configuration set name (Konfigurationssatz-Name) einen Namen für den Konfigurationssatz ein.

Note

Der Name darf maximal 64 alphanumerische Zeichen enthalten. Er darf auch Bindestriche (-) und Unterstriche (_) aufweisen. Namen dürfen keine Leerzeichen, Akzentbuchstaben oder andere Sonderzeichen enthalten.

Sie können auch mithilfe der `CreateConfigurationSet`-API Konfigurationssätze erstellen. Eine gängige Methode zum Aufrufen dieser API ist die Verwendung der AWS CLI.

So erstellen Sie einen Konfigurationssatz mithilfe der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses create-configuration-set --configuration-set Name=ConfigSet
```

Ersetzen Sie im vorherigen Befehl *ConfigSet* durch den Namen, den Sie dem Konfigurationssatz geben möchten.

Note

Der Name darf maximal 64 alphanumerische Zeichen enthalten. Er darf auch Bindestriche (-) und Unterstriche (_) aufweisen. Namen dürfen keine Leerzeichen, Akzentbuchstaben oder andere Sonderzeichen enthalten.

Weitere Informationen zur Verwendung der `CreateConfigurationSet`-API zum Erstellen von Konfigurationssätzen finden Sie in der [Amazon Simple Email Service API-Referenz](#).

Anzeigen einer Liste Ihrer Konfigurationssätze

Sie können die Amazon SES Konsole verwenden oder die Berechtigung `ListConfigurationSets`-API, um eine Liste Ihrer Konfigurationssätze anzuzeigen.

So zeigen Sie Ihre Konfigurationssätze über die Amazon SES Konsole an

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.

Im Detailbereich sehen Sie eine Liste Ihrer Konfigurationssätze.

Sie können auch mithilfe der `ListConfigurationSets`-API eine Liste der Konfigurationssätze anzeigen. Eine gängige Methode zum Aufrufen dieser API ist die Verwendung der AWS CLI.

So zeigen Sie mit der AWS CLI eine Liste der Konfigurationssätze an

- Geben Sie in der Befehlszeile folgenden Befehl ein:


```
aws ses list-configuration-sets
```

Weitere Informationen zur Verwendung von `ListConfigurationSets`-API finden Sie unter, um Ihre Konfigurationssätze aufzulisten. [Amazon Simple Email Service API-Referenz](#).

Anzeigen der Details eines Konfigurationssatzes

Sie können die Amazon SES Konsole verwenden, um die Details eines Konfigurationssatzes anzuzeigen, oder Sie verwenden die `DescribeConfigurationSet`-API, um einen Konfigurationssatz zu beschreiben.

Anzeigen der Details eines Konfigurationssatzes mit der Amazon SES Konsole

1. Melden Sie sich beim `an.AWS Management Console` und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich `Configuration Sets` aus.
3. Wählen Sie im Detailbereich das Erweitern-Symbol neben dem Konfigurationssatz.

Sie sehen die Details des Konfigurationssatzes.

Sie können die `DescribeConfigurationSet`-API auch verwenden, um weitere Informationen zu einem Konfigurationssatz anzuzeigen. Eine gängige Methode zum Aufrufen dieser API ist die Verwendung der AWS CLI.

So rufen Sie weitere Informationen über einen Konfigurationssatz mit der AWS CLI ab

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses describe-configuration-set --configuration-set-name ConfigSet
```

Ersetzen Sie im vorherigen Befehl *ConfigSet* durch den Namen des Konfigurationssatzes, über den Sie weitere Informationen abrufen möchten.

Weitere Informationen zur Verwendung der `DescribeConfigurationSet`-API verwenden, um einen Konfigurationssatz zu beschreiben, finden Sie in der [Amazon Simple Email Service API-Referenz](#).

Löschen eines Konfigurationssatzes

Sie können die Amazon SES Konsole oder die `DeleteConfigurationSet`-API verwenden, um einen Konfigurationssatz zu löschen.

So löschen Sie einen Konfigurationssatz mithilfe der Amazon SES Konsole

1. Melden Sie sich beim `an.AWS Management Console` und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich `Configuration Sets` aus.
3. Wählen Sie im Detailbereich den Konfigurationssatz.
4. Wählen Sie im Menü `Actions` die Option `Delete` und bestätigen Sie anschließend, dass Sie den Konfigurationssatz löschen möchten.

Sie können mithilfe der `DeleteConfigurationSet`-API auch Konfigurationssätze löschen. Eine gängige Methode zum Aufrufen dieser API ist die Verwendung der AWS CLI.

So löschen Sie einen Konfigurationssatz mit der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-configuration-set --configuration-set ConfigSet
```

Ersetzen Sie im vorherigen Befehl *ConfigSet* durch den Namen des Konfigurationssatzes, den Sie löschen möchten.

Weitere Informationen über die `DeleteConfigurationSet`-API zum Löschen eines Konfigurationssatzes finden Sie in der [Amazon Simple Email Service API-Referenz](#).

Verwalten von Amazon SES Standardkonfigurationssätzen

Sie können einer E-Mail-Identität einen Standardkonfigurationssatz hinzufügen, wenn Sie die Identität erstellen, oder Sie können einer vorhandenen Identität einen Standardkonfigurationssatz hinzufügen. Sie können Standardkonfigurationssätze sowohl auf E-Mail-Adresse als auch auf Domänenidentitäten anwenden.

Ein Standardkonfigurationssatz wendet seine Regeln automatisch auf alle Nachrichten an, die Sie von der E-Mail-Identität senden, die diesem Konfigurationssatz zugeordnet ist.

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.
- Eine Standardkonfiguration, die auf E-Mail-Adressebene festgelegt wurde, überschreibt eine Standardkonfiguration auf Domänenebene. Beispiel: Ein Standardkonfigurationssatz, der mit `joe@example.com` überschreibt den Konfigurationssatz für die Domäne `example.com`.
- Eine Standardkonfiguration auf Domänenebene 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 an Amazon SES mit einem Fehler „fehlerhafte Anforderung“ fehl.

Erstellen und Überprüfen einer Identität mit einer Standardkonfiguration mithilfe der Amazon SES API

Sie können die Berechtigung `CreateEmailIdentity` in der Amazon SES API v2 verwenden, um eine neue E-Mail-Identität zu erstellen und gleichzeitig den Standardkonfigurationssatz 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](#).

Zum Festlegen eines Standardkonfigurationssatzes mit der AWS CLI

- Geben Sie in der Befehlszeile den folgenden Befehl ein, um das [CreateEmailIdentity](#) verwenden.

```
aws sesv2 create-email-identity --email-identity ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Ersetzen Sie in den vorhergehenden Befehlen **ADRESSE-ODER-DOMÄNE** Sie können die E-Mail-Identität angeben, die Sie verifizieren möchten. Ersetzen **CONFIG-SATZ** Ersetzen Sie durch den Namen des Konfigurationssatzes, den Sie als Standardkonfigurationssatz für die -Identität festlegen möchten.

Bei erfolgreicher Ausführung wird der Befehl ohne Ausgabe beendet.

So überprüfen 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 **RegionName** ist der Name der AWS Region, in der Sie versucht haben, die E-Mail-Adresse zu überprüfen.

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. Klicken Sie in der Amazon SES Konsole unter **Identitätsmanagement**, wählen Sie **E-Mail-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“.

So überprüfen Sie Ihre Domäne:

Weitere Informationen zur Überprüfung Ihrer Domäne finden Sie unter [Verifizieren einer Domäne mit Amazon SES](#) (p. 66) Weitere Informationen finden Sie unter.

Hinzufügen eines Standardkonfigurationssatzes zu einer vorhandenen E-Mail-Identität mithilfe der Amazon SES API

Sie können die Berechtigung [PutEmailIdentityConfigurationSetAttributes](#) verwenden, um einen Standardkonfigurationssatz einer vorhandenen E-Mail-Identität hinzuzufügen oder 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 mit der AWS CLI

- Geben Sie in der Befehlszeile den folgenden Befehl ein, um das [PutEmailIdentityConfigurationSetAttributes](#) verwenden.

```
aws sesv2 put-email-identity-configuration-set-attributes --email-identity ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Ersetzen Sie in den vorhergehenden Befehlen **ADRESSE-ODER-DOMÄNE** Sie können die E-Mail-Identität angeben, die Sie verifizieren möchten. Ersetzen **CONFIG-SATZ** Ersetzen Sie durch den Namen des Konfigurationssatzes, den Sie als Standardkonfigurationssatz der Identität festlegen möchten.

Bei erfolgreicher Ausführung wird der Befehl ohne Ausgabe beendet.

So entfernen Sie einen Standardkonfigurationssatz mit der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein, um den Befehl `PutMailIdentityConfigurationSetAttributes` verwenden.

```
aws sesv2 put-email-identity-configuration-set-attributes --email-identity ADRESSE-OR-DOMAIN
```

Ersetzen Sie in den vorhergehenden Befehlen **ADRESSE-ODER-DOMÄNE** Sie können die E-Mail-Identität angeben, die Sie verifizieren möchten.

Bei erfolgreicher Ausführung wird der Befehl ohne Ausgabe beendet.

Zurückgeben eines Standardkonfigurationssatzes mithilfe der Amazon SES API

Sie können die Berechtigung `GetEmailIdentity`, um den Standardkonfigurationssatz für eine E-Mail-Identität zurückzugeben, falls zutreffend.

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 der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein, um den Befehl `GetEmailIdentity` verwenden.

```
aws sesv2 get-email-identity --email-identity ADRESSE-OR-DOMAIN
```

Ersetzen Sie in den vorhergehenden Befehlen **ADRESSE-ODER-DOMÄNE** mit E-Mail-Identität, für die Sie den Standardkonfigurationssatz kennen möchten, falls vorhanden.

Bei erfolgreicher Ausführung stellt der Befehl ein JSON-Objekt mit den E-Mail-Identitätsdetails bereit.

Überschreiben eines Standardkonfigurationssatzes mithilfe der Amazon SES API

Sie können die Berechtigung `SendEmail`-Vorgang, um E-Mails mit einem anderen Konfigurationssatz zu senden. Wenn Sie dies tun, überschreibt der von Ihnen angegebene Konfigurationssatz den Standardkonfigurationssatz für die Identität.

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 der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein, um den Befehl `SendEmail` verwenden.

```
aws sesv2 send-email --destination file://DESTINATION-JSON --content file://CONTENT-JSON --  
from-email-address ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Ersetzen Sie in den vorhergehenden Befehlen *ZIEL-JSON* mit Ihrer Ziel-JSON-Datei, *INHALT-JSON* mit Ihrer Content-JSON-Datei, *ADRESSE-ODER-DOMÄNE* mit Ihrer FROM-E-Mail-Adresse und *CONFIG-SATZ* Ersetzen Sie durch den Namen des Konfigurationssatzes, den Sie anstelle des Standardkonfigurationssatzes für die -Identität verwenden möchten.

Wird der Befehl erfolgreich ausgeführt, gibt er einen `MessageId`.

Verwalten von Veranstaltungszielen in Amazon SES

Mit Ereigniszielen können Sie E-Mail-Sendemetriken — einschließlich der gesendeten, angeklickten und unzustellbaren E-Mails sowie Beschwerden — in anderen AWS Produkten veröffentlichen. Weitere Informationen zum Einrichten der Ereignisveröffentlichung finden Sie unter [the section called “Überwachen des Versands mithilfe der Ereignisveröffentlichung” \(p. 313\)](#).

Aktualisieren eines Ereignisziels

Sie können die Amazon SES Konsole oder die `UpdateConfigurationSetEventDestination`-API zum Aktualisieren eines Ereignisziels.

So aktualisieren Sie ein Ereignisziel (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.
3. Wählen Sie in der Liste der Konfigurationssätze den Konfigurationssatz, der das Ereignisziel enthält, das Sie aktualisieren möchten.
4. Wählen Sie in der Liste Destination (Ziel) rechts neben dem Ziel, das Sie bearbeiten möchten, das Symbol edit (Bearbeiten) (.
5. Bearbeiten Sie die Details des Ereignisziels und klicken Sie dann auf Save.
6. Verwenden Sie die Zurück-Schaltfläche Ihres Browsers, um die Seite Edit Configuration Set zu verlassen.

Weitere Informationen zur Verwendung des `UpdateConfigurationSetEventDestination`-API zum Aktualisieren eines Ereignisziels finden Sie in der [Amazon Simple Email Service API-Referenz](#).

Löschen eines Ereignisziels

Sie können die Amazon SES Konsole oder die `DeleteConfigurationSetEventDestination`-API zum Löschen eines Ereignisziels.

So löschen Sie ein Ereignisziel (Konsole)

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.

2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.
3. Wählen Sie in der Liste der Konfigurationssätze den Konfigurationssatz, der das Ereignisziel enthält, das Sie löschen möchten.
4. Klicken Sie in der Liste Destination (Ziel) auf das Symbol delete (Löschen) (✖).
5. Bestätigen Sie, dass Sie den Konfigurationssatz löschen möchten.
6. Verwenden Sie die Zurück-Schaltfläche Ihres Browsers, um die Seite Edit Configuration Set zu verlassen.

Weitere Informationen zur Verwendung des `DeleteConfigurationSetEventDestination`-API zum Löschen eines Ereignisziels finden Sie in der [Amazon Simple Email Service API-Referenz](#).

Aktivieren oder Deaktivieren eines Ereignisziels

Sie können die Amazon SES Konsole oder die `UpdateConfigurationSetEventDestination`-API zum Aktivieren oder Deaktivieren eines Ereignisziels.

So aktivieren oder deaktivieren Sie ein Ereignisziel (Konsole)

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.
3. Wählen Sie in der Liste der Konfigurationssätze den Konfigurationssatz, der das Ereignisziel enthält, das Sie aktivieren oder deaktivieren möchten.
4. Wählen Sie in der Liste Destination rechts neben dem Ziel, das Sie bearbeiten möchten, das Bearbeiten-Symbol (den Stift).
5. Aktivieren oder deaktivieren Sie die Option Enabled und wählen Sie Save aus.
6. Verwenden Sie die Zurück-Schaltfläche Ihres Browsers, um die Seite Edit Configuration Set zu verlassen.

Weitere Informationen zur Verwendung des `UpdateConfigurationSetEventDestination`-API zum Aktivieren oder Deaktivieren eines Ereignisziels finden Sie in der [Amazon Simple Email Service API-Referenz](#).

Verwalten von dedizierten IP-

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.

So weisen Sie einen IP-Pool einem vorhandenen Konfigurationssatz zu

Mithilfe der Amazon SES -Konsole ordnen Sie einen IP-Pool einem vorhandenen Konfigurationssatz zu.

So weisen Sie einen IP-Pool einem Konfigurationssatz zu

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.

2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.
3. Wählen Sie in der Liste der Konfigurationssätze denjenigen aus, der einem IP-Pool zugeordnet werden soll.
4. Wählen Sie auf der Registerkarte Sending IP pool für Pool name eine der folgenden Optionen aus:
 - 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. Weitere Informationen zum Erstellen neuer IP-Pools finden Sie unter [Erstellen von dedizierten IP-Pools \(p. 196\)](#).
 - ses-default-dedicated-poolses-In diesem Pool befinden sich alle dedizierten IP-Adressen Ihres Kontos, die noch keinem anderen IP-Pool zugewiesen wurden. 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 im Standardpool gesendet.
 - ses-shared-poolses-Dieser Pool enthält sehr viele IP-Adressen, die für alle Amazon SES -Kunden verfügbar sind. Diese Option kann sinnvoll sein, wenn Sie E-Mails senden müssen, die nicht Ihrem üblichen Sendeverhalten entsprechen.

Wenn Sie die Auswahl getroffen haben, klicken Sie auf Assign.

Ändern von IP-Poolzuweisungen

Mit der Amazon SES -Konsole können Sie einem Konfigurationssatz, dem bereits ein Pool zugeordnet ist, auch einen anderen Pool zuweisen. Wenn Sie einem Konfigurationssatz einen anderen Pool zuweisen, wird die vorherige Zuordnung überschrieben.

So ändern Sie eine IP-Poolzuweisung

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.
3. Wählen Sie in der Liste der Konfigurationssätze denjenigen aus, den Sie ändern möchten.
4. Klicken Sie auf der Registerkarte Sending IP pool (Sender IP-Pool) unter Assign an IP pool (IP-Pool zuweisen) auf das Symbol edit (Bearbeiten) (✎).
5. Wählen Sie unter Pool name den zu verwendenden Pool aus und klicken Sie auf Assign.

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 Amazon SES E-Mail-Versandmethoden, einschließlich der [AWS CLI](#), die [AWS SDKs](#), und die [Amazon SES SMTP-Schnittstelle \(p. 94\)](#)— Ermöglicht das Übermitteln eines Konfigurationssatzes in den von Ihnen gesendeten E-Mails.

Wenn Sie die [SMTP-Schnittstelle \(p. 94\)](#) 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 Anleitung enthält Code-Beispiele für das Senden von E-Mails mittels Postfix, AWS SDKs und der Amazon SES SMTP-Schnittstelle. Jedes dieser Beispiele enthält eine Methode für das Festlegen eines Konfigurationssatzes. Schritt-für-Schritt-Anweisungen für das Senden von E-Mails, die Verweise auf Konfigurationssätzen enthalten, finden Sie unter:

- [Integrieren von Amazon SES mit Postfix \(p. 103\)](#)
- [Senden einer E-Mail über Amazon SES mithilfe eines AWS -SDKs \(p. 34\)](#)
- [So senden Sie mit SMTP eine E-Mail über Amazon SES \(p. 23\)](#)

Weitere Codebeispiele finden Sie im [Amazon SES Codebeispiele \(p. 452\)](#)-Abschnitt.

Exportieren von Zuverlässigkeitsmetriken für einen Konfigurationssatz nach CloudWatch

Amazon SES exportiert Informationen über die gesamten Unzustellbarkeits- und Beschwerdequoten für Ihr gesamtes Konto automatisch nach Amazon CloudWatch. Sie können anhand dieser Metriken Alarme in CloudWatch erstellen oder mithilfe einer Lambda Funktion das Senden von E-Mails automatisch pausieren.

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 Zuverlässigkeitsdaten für einzelne Konfigurationssätze nach CloudWatch, indem Sie die Amazon SES -API verwenden.

So aktivieren Sie den Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz

Um mit dem Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz zu beginnen, verwenden Sie die `UpdateConfigurationSetReputationMetricsEnabled`-API-Operation. Um auf die Amazon SES -API zuzugreifen, empfehlen wir die AWS CLI oder einem der AWS -SDKs.

Bei diesem Verfahren wird davon ausgegangen, dass die AWS CLI auf Ihrem Computer installiert und ordnungsgemäß konfiguriert ist. Weitere Informationen zum Installieren und Konfigurieren der AWS CLI finden Sie im [AWS Command Line Interface-Benutzerhandbuch](#).

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** im vorherigen Befehl mit den Namen des Konfigurationssatzes, für den Sie mit dem Export der Zuverlässigkeitsmetriken beginnen möchten.

So deaktivieren Sie den Export von Zuverlässigkeitsmetriken für einen Konfigurationssatz

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** im vorherigen Befehl mit den Namen des Konfigurationssatzes, für den Sie den Export der Zuverlässigkeitsmetriken deaktivieren möchten.

Überwachen Ihrer Amazon SES Versandaktivitäten

Amazon SES stellt Methoden für die Überwachung Ihrer Sendeaktivität bereit. Am besten implementieren Sie diese Methoden, damit Sie wichtige Maßnahmen – wie Ihre kontobezogenen Quoten für Unzustellbarkeit, Beschwerden und Ablehnungen – verfolgen können. Übermäßig hohe Unzustellbarkeits- und Beschwerdequoten können dazu führen, dass Sie keine E-Mails mehr mit Amazon SES senden können.

Mittels dieser Methoden können Sie auch messen, wie viele Kunden auf die von Ihnen gesendeten E-Mails reagieren, und so das Kundeninteresse quantifizieren. Beispielsweise lassen sich mit diesen Sendemetriken die allgemeinen Öffnungs- und Durchklickquoten Ihrer E-Mails ermitteln.

Die mit Amazon SES messbaren Metriken werden als E-Mail-Sendeereignisse aus. Sie können folgende E-Mail-Sendeereignisse überwachen:

- **Sends (Sendevorgänge)** Amazon SES war erfolgreich und Amazon SES wird versuchen, die E-Mail zu übermitteln.
- **Ablehnungen** Amazon SES hat die E-Mail akzeptiert, einen Virus darin erkannt und sie abgelehnt. Amazon SES hat nicht versucht, die E-Mail an den E-Mail-Server des Empfängers zu übermitteln.
- **Unzustellbarkeit** Die E-Mail wurde vom E-Mail-Server des Empfängers dauerhaft abgelehnt. Dieses Ereignis entspricht einer permanenten Unzustellbarkeit. Temporäre Unzustellbarkeiten werden nur dann aufgenommen, wenn Amazon SES über einen bestimmten Zeitraum vergeblich versucht hat, die E-Mail zuzustellen.
- **Beschwerden** Deliveries — Die E-Mail wurde erfolgreich an den Empfänger zugestellt. Der Empfänger hat die E-Mail als Spam markiert.
- **Deliveries (Zustellungen)** Amazon SES hat die E-Mail erfolgreich an den E-Mail-Server des Empfängers übermittelt.
- **Opens (Öffnungsvorgänge)** — Der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
- **Clicks (Klickvorgänge)** — Der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.
- **Rendering-Fehler** Die E-Mail wurde aufgrund eines Rendering-Problems mit der Vorlage nicht gesendet. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail mit der API-Operation [SendTemplatedEmail](#) oder [SendBulkTemplatedEmail](#) senden. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen.
- **Lieferverzögerungen** 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.

Note

So fügen Sie die hinzu `DELIVERY_DELAY`-Ereignistyp einem Ereignisziel zugewiesen ist, müssen Sie den [UpdateConfigurationSetEventDestination](#)-Vorgang in der Amazon SES API V2. Derzeit können Sie diesen Ereignistyp nicht mithilfe der Amazon SES S-Konsole einem Konfigurationssatz hinzufügen.

Sie können E-Mail-Sendeereignisse auf verschiedene Arten überwachen. Die Auswahl der Methode hängt davon ab, welcher Ereignistyp überwacht werden soll, mit welcher Granularität und Detailgenauigkeit Sie überwachen möchten und wo Amazon 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	Granularität
Amazon SES Konsole	Zustellungen und Ablehnungen	Seite der Sendestatistiken (p. 284) Amazon SES Konsole	Nur Zählung Amazon	Gesamtes AWS Konto
Amazon SES Konsole	Unzustellbarkeits- und Beschwerdequoten	Reputation Dashboard-Seite (p. 400) Amazon SES Konsole	Nur berechnete Quoten	Gesamtes AWS Konto
Amazon SES API	Zustellungen, Unzustellbarkeiten, Beschwerden und Ablehnungen	GetSendStatistics API-Operation	Nur Zählung	Gesamtes AWS Konto
Amazon CloudWatch Konsole	Sendungen, Lieferungen, Öffnungen, Klicks, Unzustellbarkeiten, Unzustellbarkeitsrate, Beschwerden, Beschwerderate und Ablehnungen	CloudWatch Konsole Note Einige Metriken werden in CloudWatch erst angezeigt, wenn das zugeordnete Ereignis eintritt. Beispielsweise werden Unzustellbarkeitsmetriken in CloudWatch erst angezeigt, wenn mindestens eine gesendete E-Mail unzustellbar ist, oder Sie mithilfe der Postfachsimulator (p. 198) aus.	Nur Zählung	Gesamtes AWS Konto
Feedback-Benachrichtigungen	Zustellungen, Unzustellbarkeiten und Beschwerden	Amazon SNS Benachrichtigung (Zustellungen,	Details zu jedem Ereignis	Gesamtes AWS Konto

Überwachungsmethode	Überwachbare Ereignisse	Datenzugriff erfolgt über	Detailgenauigkeit	Granularität
		Unzustellbarkeiten und Beschwerden) oder E-Mail (nur Unzustellbarkeiten und Beschwerden)		
Ereignisveröffentlichung	Fehler beim Senden, Zustellen, Klicken, Senden von Unzustellbarkeitsbenachrichtigungen, Beschwerden, Ablehnen und Rendering.	Amazon CloudWatch oder Amazon Kinesis Data Firehose oder Amazon SNS Benachrichtigung	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 unzustellbare und abgelehnte E-Mails oder durch die Nutzung des Amazon SES Postfachsimulators entstehen. Weitere Informationen darüber, wie Sie herausfinden können, wann die Grenze Ihrer Sendekontingente erreicht ist, finden Sie unter [Überwachen Ihrer Sendekontingente \(p. 158\)](#).

Weitere Informationen zum Verwenden der einzelnen Überwachungsmethoden finden Sie in den folgenden Themen:

- [Überwachen der Senstatistiken mithilfe der Amazon SES Konsole \(p. 284\)](#)
- [Überwachen der Nutzungsstatistiken mit der Amazon SES API \(p. 285\)](#)
- [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen \(p. 288\)](#)
- [Überwachen des E-Mail-Versands mit Amazon SES Ereignisveröffentlichung \(p. 313\)](#)

Überwachen der Senstatistiken mithilfe der Amazon SES Konsole

Sie können die Anzahl der E-Mails überwachen, die von Ihrem Konto zugestellt wurden, sowie die Anzahl der Nachrichten, die abgelehnt wurden, direkt über die Amazon SES Konsole überwachen. Die Zustellungs- und Ablehnungsraten für Ihr Konto werden auf der Seite mit den Sendestatistiken angezeigt.

Informationen zu Unzustellbarkeiten und Beschwerden finden Sie im Zuverlässigkeits-Dashboard. Weitere Informationen finden Sie unter [Überwachung Ihrer Amazon SES Absenderzuverlässigkeit \(p. 400\)](#).

So erhalten Sie eine Ansicht der Metriken für die Zustellung und Ablehnung

1. Melden Sie sich beim AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich Sending Statistics aus. Die Nutzungsstatistiken werden unter Amazon SES Metrics.
3. Doppelklicken Sie auf das Diagramm für eine beliebige Metrik, um eine Ansicht der entsprechenden Trenddaten zu erhalten. Wenn Sie auf ein Diagramm doppelklicken, können Sie den Analysezeitraum auch ändern.

Überwachen der Nutzungsstatistiken mit der Amazon SES API

Die Amazon SES API stellt die `GetSendStatistics`-Operation, 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 Sendeveruche
- 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 API-Operation `GetSendStatistics` mithilfe der AWS CLI" \(p. 285\)](#)
- [the section called "Programmgesteuertes Aufrufen der Operation `GetSendStatistics`" \(p. 286\)](#)

Aufrufen der API-Operation `GetSendStatistics` mithilfe der AWS CLI

Die einfachste Methode zum Aufrufen der API-Operation `GetSendStatistics` bietet die [AWS Command Line Interface](#) (AWS CLI).

So rufen Sie die API-Operation **`GetSendStatistics`** mithilfe der AWS CLI auf

1. Sofern noch nicht geschehen, installieren Sie die AWS CLI. Weitere Informationen finden Sie unter [„Installieren der AWS Command Line Interface“](#) im AWS Command Line Interface-Benutzerhandbuch.
2. Sofern noch nicht geschehen, konfigurieren Sie die AWS CLI zur Verwendung Ihrer AWS-Anmeldeinformationen. Weitere Informationen finden Sie unter [„Konfigurieren der AWS CLI“](#) im AWS Command Line Interface-Benutzerhandbuch.
3. Geben Sie an der Befehlszeile Folgendes ein **`aws ses get-send-statistics`**.

Ist die AWS CLI ordnungsgemäß konfiguriert, werden die Sendestatistiken im JSON-Format aufgelistet. Jedes JSON-Objekt enthält die zusammengefassten Sendestatistiken für einen Zeitraum von 15 Minuten.

Programmgesteuertes Aufrufen der Operation GetSendStatistics

Sie können auch die `GetSendStatistics` Verwenden der AWS SDKs. In diesem Abschnitt finden Sie Codebeispiele für die AWS SDKs for 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 for Go \(p. 286\)](#)
- [Codebeispiel für das AWS SDK for PHP \(p. 287\)](#)
- [Codebeispiel für das AWS SDK for Python \(Boto\) \(p. 287\)](#)
- [Codebeispiel für das AWS SDK for Ruby \(p. 287\)](#)

Note

Die Voraussetzung für diese Codebeispiele ist, dass Sie eine Datei mit gemeinsam genutzten - Anmeldeinformationen erstellt haben, die Ihre AWS -Zugriffsschlüssel-ID, den geheimen AWS -Zugriffsschlüssel und Ihre bevorzugte AWS-Region enthält. Weitere Informationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei \(p. 34\)](#).

Aufrufen von GetSendStatistics mit dem AWS SDK for 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/awsserr"
)

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.(awsserr.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)
}
```

Aufrufen von GetSendStatistics mit dem AWS SDK for 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");
}

?>
```

Aufrufen von GetSendStatistics mit dem AWS SDK for 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))
```

Aufrufen von GetSendStatistics mit dem AWS SDK for 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 Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen

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 mit Amazon SES Ereignisveröffentlichung \(p. 313\)](#).

Sie können Benachrichtigungen mithilfe der Amazon SES Konsole oder der Amazon SES API einrichten.

Themen

- [Wichtige Überlegungen \(p. 288\)](#)
- [Per E-Mail gesendete Amazon SES S-Benachrichtigungen \(p. 289\)](#)
- [Amazon SES Benachrichtigungen, die über Amazon SNS gesendet werden \(p. 292\)](#)

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 Benachrichtigungen nur für E-Mails, die von dieser Identität gesendet wurden, und 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 auch [Ereignisveröffentlichung \(p. 313\)](#) Wenn Sie Benachrichtigungen über mehrere verschiedene Arten

von Ereignissen (einschließlich Unzustellbarkeitsnachrichten, Beschwerden, Zustellungen usw.) an ein Amazon SNS -Thema oder einen Kinesis Data Firehose Stream senden.

Wenn Sie keine dieser Methoden für den Empfang von Unzustellbarkeits- und Beschwerdebenachrichtigungen einrichten, leitet Amazon SES Unzustellbarkeits- und Beschwerdebenachrichtigungen automatisch weiter an die „Return-Path“-Adresse (oder die „Source“-Adresse, wenn Sie keine „Return-Path“-Adresse angegeben haben) in der E-Mail, die das Unzustellbarkeits- und Beschwerdeereignis ausgelöst hat. 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 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.

Per E-Mail gesendete Amazon SES S-Benachrichtigungen

Amazon SES kann Ihnen eine E-Mail senden, wenn Sie Unzustellbarkeitsnachrichten und Beschwerden erhalten, indem ein Prozess namens Weiterleitung von E-Mail-Feedback.

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 [Amazon SES Benachrichtigungen, die über Amazon SNS gesendet werden \(p. 292\)](#).
- Veröffentlichen von Ereignisbenachrichtigungen. Weitere Informationen finden Sie unter [Überwachen des E-Mail-Versands mit Amazon SES Ereignisveröffentlichung \(p. 313\)](#).

Important

Wichtige Informationen zu Benachrichtigungen finden Sie unter [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen \(p. 288\)](#).

Themen

- [Aktivieren der E-Mail-Feedback-Weiterleitung \(p. 289\)](#)
- [Deaktivieren der E-Mail-Feedback-Weiterleitung \(p. 290\)](#)
- [E-Mail-Feedback-Weiterleitungsziel \(p. 291\)](#)

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 beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management die Option Email Addresses aus, wenn Sie Unzustellbarkeits- und Beschwerdebenachrichtigungen für eine E-Mail-Adresse konfigurieren möchten oder wählen Sie Domains aus, wenn Sie Unzustellbarkeits- und Beschwerdebenachrichtigungen für eine Domäne konfigurieren möchten.
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.
5. Wählen Sie Edit Configuration aus.
6. Wählen Sie unter Email Feedback Forwarding die Option Enabled aus.

Note

Bis Änderungen, die Sie auf dieser Seite vornehmen, wirksam werden, können einige Minuten vergehen.

Sie können die Unzustellbarkeits- und Beschwerdebenachrichtigungen per E-Mail auch über die [SetIdentityFeedbackForwardingEnabled](#)-API-Operation 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 beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management die Option Email Addresses aus, wenn Sie Unzustellbarkeits- und Beschwerdebenachrichtigungen für eine E-Mail-Adresse konfigurieren möchten oder wählen Sie Domains aus, wenn Sie Unzustellbarkeits- und Beschwerdebenachrichtigungen für eine Domäne konfigurieren möchten.
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.
5. Wählen Sie Edit Configuration aus.
6. Wählen Sie unter Email Feedback Forwarding die Option Disabled 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 E-Mail-Feedback deaktivieren, müssen Sie von Amazon SNS gesendete Benachrichtigungen aktivieren oder Unzustellbarkeits- und Beschwerdeereignisse in einem Amazon SNS -Thema oder einem Kinesis Data Firehose

Stream mithilfe von [Ereignisveröffentlichung](#) (p. 313). 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 weiter an die Adresse (oder das Feld „Quelle“ -Feld, 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.

Sie können die Unzustellbarkeits- und Beschwerdebenachrichtigungen per E-Mail auch über die [SetIdentityFeedbackForwardingEnabled](#)-API-Operation deaktivieren.

E-Mail-Feedback-Weiterleitungsziel

Wenn Sie Benachrichtigungen per E-Mail erhalten, schreibt Amazon SES die `From`-Header 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 gesendet haben, werden Benachrichtigungen an die Adresse geleitet, die im `MAIL FROM`-Befehl angegeben wird.

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 im Aufruf der `SendRawEmail`-API einen `Source`-Parameter angegeben haben, dann werden Benachrichtigungen an diese Adresse gesendet. Dies gilt auch, wenn Sie im Text der E-Mail eine `Return-Path`-Kopfzeile angegeben haben.
- Wenn Sie in der unformatierten Nachricht eine `Return-Path`-Kopfzeile angegeben haben, werden die 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.

Amazon SES Benachrichtigungen, die über Amazon SNS gesendet werden

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 Benachrichtigungen sind in [JavaScript Object Notation \(JSON\)](#)-Format, sodass diese programmgesteuert verarbeitet werden 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 [Per E-Mail gesendete Amazon SES S-Benachrichtigungen](#) (p. 289).
- Veröffentlichen von Ereignisbenachrichtigungen. Weitere Informationen finden Sie unter [Überwachen des E-Mail-Versands mit Amazon SES Ereignisveröffentlichung](#) (p. 313).

Important

Wichtige Informationen zu Benachrichtigungen finden Sie unter [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen](#) (p. 288).

Themen

- [Konfigurieren von Amazon SNS Benachrichtigungen für Amazon SES](#) (p. 292)
- [Amazon SNS Benachrichtigungsinhalte für Amazon SES](#) (p. 295)
- [Amazon SNS Benachrichtigungsbeispiele für Amazon SES](#) (p. 307)

Konfigurieren von Amazon SNS Benachrichtigungen für Amazon SES

Amazon SES kann Sie über Ihre Unzustellbarkeiten, Beschwerden und Zustellungen benachrichtigen. [Amazon Simple Notification Service \(Amazon SNS\)](#).

Sie können Benachrichtigungen in der Amazon SES Konsole oder mithilfe der Amazon SES-API konfigurieren.

Themen in diesem Abschnitt:

- [Prerequisites](#) (p. 292)
- [Konfigurieren von Benachrichtigungen mit der Amazon SES Konsole](#) (p. 293)
- [Konfigurieren von Benachrichtigungen mit der Amazon SES API](#) (p. 294)
- [Fehlerbehebung bei Feedback-Benachrichtigungen](#) (p. 295)

Prerequisites

Führen Sie die folgenden Schritte aus, bevor Sie Amazon SNS Benachrichtigungen in Amazon SES einrichten:

1. Erstellen eines Themas in Amazon SNS. Weitere Informationen finden Sie unter [Erstellen eines Themas](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

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 finden Sie unter [Erste Schritte](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

3. (Optional) Wenn Ihr Amazon SNS -Thema AWS Key Management Service (AWS KMS) für die serverseitige Verschlüsselung müssen Sie Berechtigungen zur AWS KMS Schlüsselrichtlinie. Sie können Berechtigungen hinzufügen, indem Sie die folgende Richtlinie an die AWS KMS-Schlüsselrichtlinie anfügen:

```
{
  "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 Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich unter Identity Management entweder Domains oder Email Addresses aus.
3. Wählen Sie in der Liste der verifizierten Sender die E-Mail-Adresse oder Domäne aus, für die Benachrichtigungen konfiguriert werden sollen.

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 unter Notifications die Option Edit Configuration aus.
5. **UNDERSNS-Thema** Nehmen Sie die folgenden Änderungen an der Konfiguration des Amazon SNS-Themas vor:
 - a. Wählen Sie die Amazon SNS -Themen aus, die Sie zum Empfang von Benachrichtigungen verwenden wollen. Sie können mehrere Ereignistyp-Benachrichtigungen im gleichen Amazon SNS -Thema oder in verschiedenen Amazon SNS-Themen veröffentlichen.

Important

Die Amazon SNS -Themen, die Sie für Unzustellbarkeits-, Beschwerde- und Zustellungsnachrichten einsetzen, müssen sich in derselben AWS Region befinden, in der 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 finden Sie unter [Erste Schritte](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

Wenn Sie ein Amazon SNS -Thema verwenden möchten, das Sie nicht besitzen, müssen Sie [So konfigurieren Sie Ihren AWS Identity and Access Management \(IAM\) -Richtlinie](#). So ermöglichen Sie die Veröffentlichung des Amazon-Ressourcennamens (ARN) des Amazon SNS -Themas.

- b. Wenn die Amazon SNS Benachrichtigungen die ursprünglichen Header der an Amazon SES übergebenen E-Mails enthalten sollen, wählen Sie [Einschließen der ursprünglichen Header](#). 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 [Amazon SNS Benachrichtigungsinhalte \(p. 295\)](#).
6. (Optional) Wenn Sie Amazon SNS -Themen sowohl für Unzustellbarkeiten als auch für Beschwerden ausgewählt haben, können Sie die E-Mail-Benachrichtigungen vollständig deaktivieren. Zum Deaktivieren der E-Mail-Benachrichtigungen für Unzustellbarkeiten und Beschwerden wählen Sie unter Email Feedback Forwarding die Option Disable aus. Benachrichtigungen zur Zustellung stehen nur über Amazon SNS zur Verfügung.
7. Wählen Sie Save Config aus. Es kann ein paar Minuten dauern, bis die Änderungen an den Benachrichtigungseinstellungen übernommen werden.

Nachdem Sie Ihre Einstellungen konfiguriert haben, werden die Unzustellbarkeits-, Beschwerde- und Zustellungsbenachrichtigungen an Ihre Amazon SNS -Themen gesendet. Diese Benachrichtigungen weisen das JavaScript Object Notation (JSON)-Format und die unter [Amazon SNS Benachrichtigungsinhalte \(p. 295\)](#) beschriebene Struktur auf.

Für Unzustellbarkeits-, Beschwerde- und Zustellungsbenachrichtigungen werden die Amazon SNS -Standardgebühren erhoben. Weitere Informationen finden Sie im [Amazon SNS Preisseite](#).

Note

Wenn ein Versuch, in Ihrem Amazon SNS -Thema zu veröffentlichen, fehlschlägt, weil das Thema gelöscht wurde oder Ihr AWS Konto nicht mehr über die Berechtigungen zum Veröffentlichen verfügt, entfernt Amazon SES die Konfiguration für dieses Thema. Darüber hinaus Amazon SES Benachrichtigungen über Unzustellbarkeits- und Beschwerdebenachrichtigungen 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 unter [Amazon Simple Email Service-API-Referenz](#).

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 finden Sie unter [Erste Schritte](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

InvalidParameterValue-Fehler beim Auswählen eines Themas

Wenn Sie einen Fehler erhalten, der besagt, dass ein **InvalidParameterValue**-Fehler aufgetreten ist, überprüfen Sie das Amazon SNS -Thema, um zu sehen, ob es mit AWS KMS. Wenn dies der Fall ist, müssen Sie die Richtlinie für den AWS KMS-Schlüssel abändern. Eine Beispielrichtlinie finden Sie unter [Prerequisites](#) (p. 292).

Amazon SNS Benachrichtigungsinhalte für Amazon SES

Benachrichtigungen zur Unzustellbarkeit, zu Beschwerden und zur Zustellung werden auf veröffentlicht [Amazon Simple Notification Service \(Amazon SNS\)](#)-Themen im JavaScript Object Notation (JSON) -Format. 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](#) (p. 296)
- [mail-Objekt](#) (p. 296)
- [bounce-Objekt](#) (p. 299)
- [complaint-Objekt](#) (p. 304)
- [delivery-Objekt](#) (p. 306)

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. Der Code sollte in der Lage sein, die Amazon SNS -Benachrichtigung zu analysieren und beide Fälle verarbeiten können. Amazon SES macht keine Anordnungs- oder Stapelverarbeitung für Benachrichtigungen über Amazon SNS. Unterschiedliche Amazon SNS Benachrichtigungstypen (beispielsweise Unzustellbarkeit und Beschwerden) werden jedoch nie 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.
- Amazon SES behält sich das Recht vor, zusätzliche Felder in die Benachrichtigungen einzufügen. Deshalb müssen Anwendungen, die diese Benachrichtigungen analysieren, in der Lage sein, unbekannte Felder zu verarbeiten.
- Amazon SES überschreibt die Header 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 Amazon SES Benachrichtigung enthält die folgenden Felder.

Feldname	Beschreibung
<code>notificationType</code>	Eine Zeichenfolge, die den Typ der Benachrichtigung enthält, der vom JSON-Objekt dargestellt wird. Die möglichen Werte sind <code>Bounce</code> , <code>Complaint</code> oder <code>Delivery</code> .
<code>mail</code>	Ein JSON-Objekt, das Informationen zur ursprünglichen E-Mail enthält, auf die sich die Benachrichtigung bezieht. Weitere Informationen finden Sie unter Mail-Objekt (p. 296) .
<code>bounce</code>	Dieses Feld ist nur dann vorhanden, wenn <code>notificationType</code> <code>Bounce</code> ist, und enthält ein JSON-Objekt mit Informationen über die Unzustellbarkeit. Weitere Informationen finden Sie unter Bounce-Objekt (p. 299) .
<code>complaint</code>	Dieses Feld ist nur dann vorhanden, wenn <code>notificationType</code> <code>Complaint</code> ist, und enthält ein JSON-Objekt mit Informationen zur Beschwerde. Weitere Informationen finden Sie unter Complaint-Objekt (p. 304) .
<code>delivery</code>	Dieses Feld ist nur dann vorhanden, wenn <code>notificationType</code> <code>Delivery</code> ist, und enthält ein JSON-Objekt mit Informationen zur Zustellung. Weitere Informationen finden Sie unter Delivery-Objekt (p. 306) .

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	Beschreibung
<code>timestamp</code>	Der Zeitpunkt, zu dem die ursprüngliche Nachricht gesendet wurde (im ISO8601-Format).
<code>messageId</code>	Eine eindeutige ID, die Amazon SES der Nachricht zugewiesen hat. Amazon SES diesen Wert an Sie zurück, wenn Sie die Nachricht gesendet haben. Note Amazon SES hat diese Nachrichten-ID zugewiesen. Sie finden diese in der ursprünglichen E-Mail in den Feldern <code>headers</code> und <code>commonHeaders</code> des Objekts <code>mail</code> .

Feldname	Beschreibung
<code>source</code>	Die E-Mail-Adresse, von der die ursprüngliche Nachricht gesendet wurde (die Envelope-MAIL-FROM-Adresse).
<code>sourceArn</code>	Der Amazon-Ressourcenname (ARN) der Identität, die zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt <code>sourceArn</code> den ARN der ID an, die – gemäß Autorisierung durch den Identitätseigentümer – vom stellvertretenden Sender zum Senden der E-Mail verwendet werden soll. Weitere Informationen zur Sendeautorisierung finden Sie unter Verwenden der Sendeautorisierung (p. 162) .
<code>sourceIp</code>	Die ursprüngliche öffentliche IP-Adresse des Clients, der Anforderung zum Senden der E-Mail an Amazon SES durchgeführt hat.
<code>sendingAccountId</code>	Die AWS-Konto-ID des Kontos, das zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt <code>sendingAccountId</code> die Konto-ID des stellvertretenden Senders an.
<code>destination</code>	Eine Liste der E-Mail-Adressen, an die die ursprüngliche E-Mail gesendet wurde.
<code>headersTruncated</code>	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. Amazon SES kürzt die Header in der Benachrichtigung, wenn die Header der ursprünglichen Nachricht mindestens 10 KB umfassen. Mögliche Werte sind <code>true</code> und <code>false</code>.
<code>headers</code>	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 <code>name</code> und <code>value</code>. Note Jede Nachrichten-ID innerhalb des <code>headers</code>-Objekt stammt von der ursprünglichen Nachricht, die Sie an Amazon SES übergeben haben. Die Nachrichten-ID, die Amazon SES der Nachricht zugewiesen hat, befindet sich im <code>messageId</code>-Feld des <code>mail</code>-Objekt.

Feldname	Beschreibung
<code>commonHeaders</code>	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 Objekts ist jeder Header ein Schlüssel. Die Absender- und Empfängerfelder werden durch Arrays repräsentiert, die mehrere Werte enthalten. Note Jede Nachrichten-ID innerhalb des <code>commonHeaders</code>-Objekts stammt von der ursprünglichen Nachricht, die Sie an Amazon SES übergeben haben. Die Nachrichten-ID, die Amazon SES der Nachricht zugewiesen hat, befindet sich im <code>messageId</code>-Feld des <code>mail</code>-Objekts.

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-west-2:888888888888: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 Amazon SES"
    }
  }
}
```

Bounce-Objekt

Das JSON-Objekt, das Informationen zu Unzustellbarkeiten enthält, weist die folgenden Felder auf.

Feldname	Beschreibung
bounceType	Der Unzustellbarkeitstyp, wie er von Amazon SES festgelegt wurde. Weitere Informationen finden Sie unter Unzustellbarkeitstypen (p. 301) .
bounceSubType	Der untergeordnete Typ der Unzustellbarkeit, wie er von Amazon SES festgelegt wurde. Weitere Informationen finden Sie unter Unzustellbarkeitstypen (p. 301) .
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 (p. 300) .
timestamp	Datum und Uhrzeit der Benachrichtigung über die Unzustellbarkeit (im ISO8601-Format). Beachten Sie, dass es sich dabei um den Zeitpunkt handelt, zu dem die Benachrichtigung vom ISP gesendet wurde, und nicht um den Zeitpunkt, zu dem diese von Amazon SES empfangen wurde.
feedbackId	Eine eindeutige ID für die Unzustellbarkeit.

Konnte Amazon SES die Remote Message Transfer Authority (MTA) erreichen, sind zudem folgende Felder enthalten.

Feldname	Beschreibung
remoteMtaIp	Die IP-Adresse der MTA, an die Amazon SES versucht hat, die E-Mail zuzustellen.

Wurde der Unzustellbarkeitsbenachrichtigung eine Zustellungsstatusbenachrichtigung (DSN, Delivery Status Notification) angefügt, ist auch das folgende Feld enthalten.

Feldname	Beschreibung
reportingMTA	Der Wert des <code>Reporting-MTA</code> -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	Beschreibung
emailAddress	Die E-Mail-Adresse des Empfängers. Ist eine DSN verfügbar, ist dies der Wert des <code>Final-Recipient</code> -Felds der DSN.

Wurde eine DSN an eine Unzustellbarkeitsbenachrichtigung angehängt, sind möglicherweise folgende Felder ebenfalls vorhanden.

Feldname	Beschreibung
<code>action</code>	Der Wert des <code>Action</code> -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.
<code>status</code>	Der Wert des <code>Status</code> -Felds der DSN. Dies ist der vom Transport unabhängige Statuscode pro Empfänger, der den Zustellstatus der Nachricht anzeigt.
<code>diagnosticCode</code>	Der vom berichtenden MTA gemeldete Statuscode. Dies ist der Wert des <code>Diagnostic-Code</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 Unzustellbarkeitsobjekt enthält eine Unzustellbarkeitsnachricht des Typs `Undetermined`, `Permanent` oder `Transient`. Die Unzustellbarkeitstypen `Permanent` und `Transient` können auch eine von mehreren Unzustellbarkeitsunterarten enthalten.

Wenn Sie eine Unzustellbarkeitsbenachrichtigung mit einer Unzustellbarkeit des Typs `Transient` erhalten, sind Sie möglicherweise in der Lage zum zukünftigen Senden von E-Mails an diesen Empfänger, wenn das Problem, das dazu führte, dass die Nachricht als unzustellbar eingestuft wurde, gelöst ist.

Wenn Sie eine Unzustellbarkeitsbenachrichtigung mit einer Unzustellbarkeit des Typs `Permanent` erhalten, ist es unwahrscheinlich, dass Sie in Zukunft 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 einTemporäre UnzustellbarkeitWenn eine temporäre Unzustellbarkeit in Bezug auf ein temporäres Problem auftritt, wie z. B. einen vollen Posteingang des Empfängers), versucht Amazon SES für einen bestimmten Zeitraum, die E-Mail erneut zuzustellen. Wenn nach Ablauf dieses Zeitraums Amazon SES die E-Mail immer noch nicht zustellen kann, werden keine weiteren Versuche mehr unternommen.

Amazon SES stellt Benachrichtigungen für permanente Unzustellbarkeiten sowie für nicht zustellbare Unzustellbarkeiten bereit, bei denen keine Zustellversuche mehr unternommen wurden. Wenn Sie jedes Mal eine Benachrichtigung erhalten möchten, wenn eine temporäre Unzustellbarkeit auftritt, [aktivieren Sie die Ereignisveröffentlichung \(p. 315\)](#) und konfigurieren Sie sie so, dass Benachrichtigungen gesendet werden, wenn Zustellungsverzögerungsereignisse auftreten.

bounceType	bounceSubType	Beschreibung
Undetermined	Undetermined	Der E-Mail-Anbieter des Empfängers hat eine Unzustellbarkeitsnachricht gesendet. Die Unzustellbarkeitsnachricht hat nicht genügend Informationen für Amazon SES enthalten, um den Grund für die Unzustellbarkeit zu ermitteln. Die Unzustellbarkeits-E-Mail, die an die Adresse im Return-Path-Header der E-Mail gesendet wurde, die zur Unzustellbarkeit geführt hat, enthält möglicherweise zusätzliche Informationen zum Problem, das die Unzustellbarkeit der E-Mail verursacht hat.
Permanent	General	Der E-Mail-Anbieter des Empfängers hat eine permanente Unzustellbarkeitsnachricht gesendet, aber keinen Grund für die permanente Unzustellbarkeit angegeben. Important Wenn Sie diese Art von Unzustellbarkeitsbenachrichtigung erhalten, sollten Sie die E-Mail-Adresse des Empfängers sofort aus Ihrer Mailingliste entfernen. Das Senden von Nachrichten 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, vorübergehend unterbrechen.
Permanent	NoEmail	Der E-Mail-Anbieter des vorgesehenen Empfängers hat eine Unzustellbarkeitsnachricht gesendet, die darauf hinweist, dass die E-Mail-Adresse nicht vorhanden ist. Important Wenn Sie diese Art von Unzustellbarkeitsbenachrichtigung erhalten, sollten Sie die E-Mail-Adresse des Empfängers sofort aus Ihrer Mailingliste entfernen. Das Senden von Nachrichten an Adressen, die nicht vorhanden sind, kann negative Auswirkungen auf Ihren guten Ruf als Absender haben. Wenn Sie weiter E-Mails an Adressen senden, die nicht vorhanden sind, können wir Ihre Fähigkeit, weitere E-Mails zu senden, vorübergehend unterbrechen.
Permanent	Suppressed	Die E-Mail-Adresse des Empfängers befindet sich auf der Amazon SES Unterdrückungsliste, da

bounceType	bounceSubType	Beschreibung
		bereits mehrere permanente Unzustellbarkeiten erzeugt wurden. Informationen zum Entfernen einer Adresse aus der -Unterdrückungsliste von Amazon SES finden Sie unter Verwenden der globalen Unterdrückungsliste von Amazon SES (p. 210) .
Permanent	OnAccountSuppressionList	Das Senden an diese Adresse hat Amazon SES unterdrückt, da sie sich auf der Registerkarte Unterdrückungsliste auf Kontoebene (p. 201) .
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 Antwortregel (z. B. eine "außer Haus"-Abwesenheitsnachricht) verfügt, erhalten Sie möglicherweise diese Art von Benachrichtigung. Obwohl die Antwort den Benachrichtigungstyp <code>Bounce</code> Wenn Amazon SES die Unzustellbarkeitsquote für Ihr Konto berechnet, zählt Amazon SES 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.
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.

bounceType	bounceSubType	Beschreibung
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 bestimmten 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	Beschreibung
complainedRecipients	Eine Liste mit Informationen zu Empfängern, die möglicherweise für die Beschwerde verantwortlich sind. Weitere Informationen finden Sie unter Empfänger, die sich beschwert haben (p. 305) .
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 ist möglicherweise nicht dasselbe wie das Datum und die Uhrzeit, als Amazon SES die Benachrichtigung empfangen hat.
feedbackId	Eine eindeutige ID, die mit der Beschwerde verknüpft ist.
complaintSubType	Der Wert des Feldes <code>complaintSubType</code> kann entweder null oder <code>OnAccountSuppressionList</code> sein. Wenn der Wert <code>OnAccountSuppressionList</code> ist, hat Amazon SES die Nachricht akzeptiert, aber nicht versucht, sie zu senden, da sie sich auf der Unterdrückungsliste auf Kontoebene (p. 201) befindet.

Ist zudem ein Feedback-Bericht an die Beschwerde angehängt, sind möglicherweise die folgenden Felder vorhanden.

Feldname	Beschreibung
userAgent	Der Wert des <code>User-Agent</code> -Felds aus dem Feedback-Bericht. Gibt den Namen und die Version des Systems an, das den Bericht generiert hat.
complaintFeedbackType	Der Wert des <code>Feedback-Type</code> -Felds aus dem Feedback-Bericht, der vom ISP empfangen wurde. Enthält die Art des Feedbacks.

Feldname	Beschreibung
arrivalDate	Der Wert des Arrival-Date-Felds oder des Received-Date-Felds 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. Sie sollten diese Informationen verwenden, um zu bestimmen, welcher Empfänger die Beschwerde erhoben hat, und dann sofort den Empfänger aus Ihren Mailinglisten entfernen.

Important

Die meisten ISPs entfernen die E-Mail-Adresse des Empfängers, der sich beschwert 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. Amazon SES führt einen Abgleich mit der ursprünglichen Nachricht durch, um diese Empfängerliste festzulegen.

JSON-Objekte in dieser Liste enthalten das folgende Feld.

Feldname	Beschreibung
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 [Internet Assigned Numbers Authority-Website](#) 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	Beschreibung
<code>timestamp</code>	Der Zeitpunkt, zu dem Amazon SES die E-Mail an den Mail-Server des Empfängers übermittelt hat (im ISO8601-Format).
<code>processingTimeMillis</code>	Der Zeitraum (in Millisekunden) zwischen dem Akzeptieren der Anforderung des Absenders seitens Amazon SES und dem Übermitteln der Nachricht an den Mail-Server des Empfängers.
<code>recipients</code>	Eine Liste der beabsichtigten Empfänger der E-Mail, für die die Zustellungsbenachrichtigung gilt.
<code>smtpResponse</code>	Die SMTP-Antwort des Remote-ISP, der die E-Mail von Amazon SES zugelassen hat. Diese Nachricht variiert je nach E-Mail, empfangendem Mail-Server und empfangendem ISP.
<code>reportingMTA</code>	Der Hostname des Amazon SES Mail-Servers, der die E-Mail gesendet hat.
<code>remoteMtaIp</code>	Die IP-Adresse der MTA, an die Amazon 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 Amazon SNS Unzustellbarkeitsbenachrichtigungen](#) (p. 307).
- Beispiele für Beschwerdebenachrichtigungen finden Sie unter [Beispiele Amazon SNS Beschwerdebenachrichtigungen](#) (p. 309).
- Beispiele für Zustellungsbenachrichtigungen finden Sie unter [Beispiel einer Amazon SNS Zustellungsbenachrichtigung](#) (p. 312).

Beispiele 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-west-2:888888888888:identity/example.com",
    "sourceIp": "127.0.3.0",
    "sendingAccountId": "123456789012",
    "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>,"
    },
    {
        "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"
    ],
    "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-west-2:888888888888:identity/example.com",
"sourceIp": "127.0.3.0",
"sendingAccountId": "123456789012",
"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 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-west-2:888888888888:identity/example.com",
    "sourceIp": "127.0.3.0",
    "sendingAccountId": "123456789012",
    "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-west-2:888888888888:identity/example.com",
    "sourceIp":"127.0.3.0",
    "sendingAccountId":"123456789012",
    "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-west-2:888888888888:identity/example.com",
    "sourceIp": "127.0.3.0",
    "sendingAccountId": "123456789012",
    "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"
}
}
```

Überwachen des E-Mail-Versands mit Amazon SES Ereignisveröffentlichung

Damit Sie den E-Mail-Versand detailliert nachverfolgen können, können Sie Amazon SES so einrichten, dass sie E-Mail-Sendeereignisse je nachdem, welche Merkmale Sie definieren, an Amazon CloudWatch, Amazon Kinesis Data Firehose oder Amazon Simple Notification Service gesendet haben.

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. Beispielsweise können Sie Ihre E-Mail-Sendedaten in CloudWatch veröffentlichen und Dashboards erstellen, die die Performance Ihrer E-Mail-Kampagnen nachverfolgen. Oder Sie können mithilfe von Amazon SNS Benachrichtigungen senden, wenn bestimmte Ereignisse eintreten.

Funktionsweise der -Ereignisveröffentlichung

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. Jedes Mal, wenn Sie dann eine E-Mail senden, geben Sie den Namen des Konfigurationssatzes und einen oder mehrere Nachrichten-Tags in Form von Name/Wert-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 Schnittstelle zum Senden von E-Mails Sie verwenden, können Sie den Nachrichten-Tag entweder als Parameter für den API-Aufruf oder als Amazon SES-spezifischen E-Mail-Header angeben. Weitere Informationen zu Konfigurationssätzen finden Sie unter [Verwenden von Amazon SES Konfigurationssätzen \(p. 271\)](#).

Zusätzlich zu den Nachrichten-Tags, die Sie angeben, fügt Amazon SES auch hinzuauto-tagsan die Nachrichten, die Sie senden. Sie müssen keine weiteren Schritte zum Verwenden der automatischen Tags durchführen.

In der folgenden Tabelle werden die automatischen Tags aufgelistet, die automatisch auf von Ihnen gesendete Nachrichten mit Amazon SES angewendet werden.

Automatische Tags von Amazon SES

Automatische Tag-Namen	Beschreibung
<code>ses:configuration-set</code>	Der Name des Konfigurationssatzes, der der E-Mail zugeordnet ist.
<code>ses:caller-identity</code>	Die IAM-Identität des Amazon SES Benutzers, der die E-Mail gesendet hat.
<code>ses:from-domain</code>	Die Domäne der "From"-Adresse.
<code>ses:source-ip</code>	Die IP-Adresse, die der Aufrufer zum Senden der E-Mail verwendet hat.
<code>ses:outgoing-ip</code>	Die IP-Adresse, die Amazon SES zum Senden der E-Mail verwendet hat.

Verwenden der Ereignisveröffentlichung

Die folgenden Abschnitte enthalten die Informationen, die Sie für die Einrichtung und Verwendung der Amazon SES Ereignisveröffentlichung benötigen.

- [Einrichten der -Ereignisveröffentlichung \(p. 315\)](#)
- [Arbeiten mit Ereignisdaten von \(p. 325\)](#)
- [Tutorials \(p. 369\)](#)

Terminologie zu Ereignisveröffentlichung

In der folgenden Liste werden Begriffe im Zusammenhang mit der -Ereignisveröffentlichung definiert.

E-Mail-Sendeereignis

Informationen im Zusammenhang mit dem Ergebnis einer E-Mail, die Sie an Amazon SES senden. Das Senden von Ereignissen umfasst Folgendes:

- **Sends (Sendevorgänge)**Send — der Anruf an Amazon SES war erfolgreich und Amazon SES wird versuchen, die E-Mail zu übermitteln.
- **Ablehnungen**— Amazon SES hat die E-Mail zunächst akzeptiert, dann jedoch einen Virus darin erkannt und die E-Mail abgelehnt. Amazon SES hat nicht versucht, die E-Mail an den E-Mail-Server des Empfängers zu senden.
- **Unzustellbarkeit**Der Mail-Server des Empfängers hat die E-Mail dauerhaft abgelehnt. Dieses Ereignis entspricht einer permanenten Unzustellbarkeit. Temporäre Unzustellbaritäten werden nur dann aufgenommen, wenn Amazon SES über einen bestimmten Zeitraum vergeblich versucht hat, die E-Mail zuzustellen.

- **Beschwerden**— Die E-Mail wurde erfolgreich an den Empfänger zugestellt. Der Empfänger hat die E-Mail als Spam markiert.
- **Deliveries (Zustellungen)Delivery** — Amazon SES hat die E-Mail erfolgreich an den E-Mail-Server des Empfängers übermittelt.
- **Opens (Öffnungsvorgänge)**Der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
- **Clicks (Klickvorgänge)**— Der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.
- **Rendering-FehlerRendering-Problems** der Vorlage wurde aufgrund eines Rendering-Problems der Vorlage nicht gesendet. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail mit der API-Operation [SendTemplatedEmail](#) oder [SendBulkTemplatedEmail](#) senden. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen.
- **Verzögerungen durch LieferungenDelivery** — 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.

Note

So fügen Sie die `hinzudeLIVERY_DELAY`Um den -Ereignistyp einem Ereignisziel hinzuzufügen, müssen Sie den [UpdateConfigurationSetEventDestination](#)Der Vorgang in der Amazon SES API V2. Derzeit können Sie diesen Ereignistyp nicht mithilfe der Amazon SES S-Konsole einem Konfigurationssatz hinzufügen.

Konfigurationssatz

Eine Gruppe von Regeln, die das Ziel definiert, an dem Amazon SES E-Mail-Sendeereignisse veröffentlicht, und die Typen von E-Mail-Sendeereignissen, 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 -Service, an den Sie Amazon SES E-Mail-Sendeereignisse veröffentlichen. Jedes eingerichtete Ereignisziel gehört zu einem einzigen Konfigurationssatz.

Nachrichten-Tag

Ein Name/Wert-Paar, mit dem Sie eine E-Mail zum Zweck der Ereignisveröffentlichung kategorisieren. Beispiele sind Kampagne/Buch und Kampagne/Bekleidung. Wenn Sie eine E-Mail senden, können Sie den Nachrichten-Tag entweder als Parameter für den API-Aufruf oder als Amazon SES-spezifischen E-Mail-Header angeben.

Automatisches Tag

Nachrichten-Tags, die automatisch in Berichten zur Ereignisveröffentlichung enthalten sind. Es gibt einen automatischen Tag für den Namen des Konfigurationssatzes, die Domäne der „From“-Adresse, die ausgehende IP-Adresse des Aufrufers, die ausgehende Amazon SES S-IP-Adresse und die IAM-Identität des Aufrufers.

Einrichten der Veröffentlichung Amazon SES Ereignissen

In diesem Abschnitt wird beschrieben, wie Sie Amazon SES so konfigurieren müssen, dass die E-Mail-Sendeereignisse in Amazon CloudWatch, Amazon Kinesis Data Firehose oder Amazon Simple Notification Service (Amazon SNS) veröffentlicht werden.

Zuerst erstellen Sie eineKonfigurationssatzmithilfe der Amazon SES Konsole oder -API. Nachdem Sie einen Konfigurationssatz erstellt haben, fügen Sie mindestens einen Konfigurationssatz hinzuVeranstaltungsziele(CloudWatch, Kinesis Data Firehose oder Amazon SNS) an den

Konfigurationssatz übergeben und konfigurieren Sie für das Ereignisziel eindeutige Parameter. Jedes Mal, wenn Sie eine E-Mail senden, geben Sie an, welcher Konfigurationssatz verwendet werden soll.

Themen in diesem Abschnitt

- [Schritt 1: Erstellen eines Konfigurationssatzes \(p. 316\)](#)
- [Schritt 2: Hinzufügen eines Ereignisziels \(p. 316\)](#)
- [Schritt 3: Festlegen eines Konfigurationssatzes für den Versand von E-Mail \(p. 323\)](#)

Schritt 1: Erstellen eines Konfigurationssatzes

Mithilfe von Konfigurationssätzen können Sie E-Mail-Sendeereignisse (Unzustellbarkeiten, Beschwerden, Zustellungen, gesendete E-Mails, abgelehnte E-Mails, Rendering-Fehler und Lieferverzögerungen) in Amazon CloudWatch oder Amazon Kinesis Data Firehose veröffentlichen.

Sie können Konfigurationssätze auch über die Amazon SES Konsole oder den [CreateConfigurationSet](#) Der Vorgang in der Amazon SES API V2.

So erstellen Sie einen Konfigurationssatz mithilfe der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich Configuration Sets aus.
3. Wählen Sie im Inhaltsbereich Create Configuration Set aus.
4. Geben Sie einen Namen für den Konfigurationssatz ein und wählen Sie Create Configuration Set aus.
5. Klicken Sie auf Close.

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 -Service-Ziel aus und legen Parameter fest, die mit diesem Ziel verknüpft sind.

Beim Einrichten eines -Ereignisziels können Sie Ereignisse an einen der folgenden AWS -Services senden: Amazon CloudWatch, Amazon Kinesis Data Firehose und 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. Wünschen Sie detaillierte Ereignisdatensätze, die Sie an einen anderen Service wie Amazon Elasticsearch Service oder Amazon Redshift für Analysen ausgeben möchten, können Sie Kinesis Data Firehose verwenden. Falls Sie Benachrichtigungen erhalten möchten, wenn bestimmte Ereignisse eintreten, verwenden Sie Amazon SNS.

In diesem Abschnitt werden folgende Themen beschrieben

- [Einrichten eines -CloudWatch Ereignisziels für die -Ereignisveröffentlichung \(p. 316\)](#)
- [Einrichten eines Kinesis Data Firehose Ereignisziels für die Veröffentlichung von Amazon SES Ereignissen \(p. 319\)](#)
- [Einrichten eines -Amazon SNS Ereignisziels für die -Ereignisveröffentlichung \(p. 322\)](#)

Einrichten eines -CloudWatch Ereignisziels für die -Ereignisveröffentlichung

Sie können Amazon CloudWatch Ereigniszielen verwenden, um Amazon SES E-Mails mit Ereignissen an CloudWatch zu veröffentlichen. Da ein CloudWatch Ereignisziel nur innerhalb eines Konfigurationssatzes

vorhanden ist, müssen Sie zuerst [Erstellen eines Konfigurationssatzes \(p. 316\)](#) So fügen Sie das - Ereignisziel zum Konfigurationssatz hinzu.

Wenn Sie einem Konfigurationssatz ein CloudWatch Ereignisziel hinzufügen, müssen Sie mindestens ein CloudWatch auswählen-Dimensionen Die den Nachrichten-Tags entsprechen, die Sie beim Senden Ihrer E-Mails verwenden. Wie Nachrichten-Tags ist auch eine CloudWatch Dimension ein Name-Wert-Paar, mit dem Sie eine Metrik eindeutig identifizieren können.

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-Sendeereignisse in CloudWatch veröffentlichen, ist es wichtig, dass Sie Ihre Nachrichten-Tags und Dimensionen auswählen. Diese Auswahl hat Auswirkungen auf die CloudWatch-Fakturierung und bestimmt, wie die Ereignisdaten Ihres E-Mail-Versands in CloudWatch gefiltert werden.

In diesem Abschnitt werden Informationen zur Unterstützung der Auswahl Ihrer Dimensionen bereitgestellt. Anschließend wird außerdem gezeigt, wie Sie einem Konfigurationssatz ein CloudWatch Ereignisziel hinzufügen.

Themen in diesem Abschnitt

- [Hinzufügen eines CloudWatch Ereignisziels \(p. 317\)](#)
- [Auswählen von CloudWatch Dimensionen \(p. 319\)](#)

Hinzufügen eines CloudWatch Ereignisziels

Das Verfahren in diesem Abschnitt veranschaulicht, wie ein CloudWatch Ereignisziel zum einem Konfigurationssatz hinzugefügt wird.

Sie können auch die [UpdateConfigurationSetEventDestination](#)-Vorgang in der Amazon SES API V2 von, um Ereignisziele zu erstellen und zu ändern.

So fügen Sie einem Konfigurationssatz mithilfe der Konsole ein CloudWatch Ereignisziel zu einem CloudWatch-Ereignisziel hinzu

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich Configuration Sets aus.
3. Wählen Sie in der Liste der Konfigurationssätze den Konfigurationssatz aus, für den Sie ein CloudWatch Ereignisziel erstellen möchten. Wenn diese Liste leer ist, müssen Sie zuerst [einen Konfigurationssatz erstellen \(p. 316\)](#).
4. Klicken Sie auf der Veranstaltungsziele Registerkarte für Ziel hinzufügen, wählen Sie Wählen Sie einen Zieltyp Klicken Sie auf und danach auf CloudWatch.
5. Klicken Sie auf der CloudWatch Ziel Wählen Sie im Dialogfeld Enabled.
6. Geben Sie im Feld Name einen Namen für das Ereignisziel ein.
7. Wählen Sie für Event types die Ereignistypen aus, die Sie im Ereignisziel veröffentlichen möchten. Die folgenden Ereignistypen sind verfügbar:
 - Sends (Sendevorgänge) Send — der Anruf an Amazon SES war erfolgreich und Amazon SES wird versuchen, die E-Mail zu übermitteln.
 - Ablehnungen — Amazon SES hat die E-Mail zunächst akzeptiert, dann jedoch einen Virus darin erkannt und die E-Mail abgelehnt. Amazon SES hat nicht versucht, die E-Mail an den E-Mail-Server des Empfängers zu senden.
 - Unzustellbarkeit Der Mail-Server des Empfängers hat die E-Mail dauerhaft abgelehnt. Dieses Ereignis entspricht einer permanenten Unzustellbarkeit. Temporäre Unzustellbaritäten werden nur dann aufgenommen, wenn Amazon SES über einen bestimmten Zeitraum vergeblich versucht hat, die E-Mail zuzustellen.

- **Beschwerden**— Die E-Mail wurde erfolgreich an den Empfänger zugestellt. Der Empfänger hat die E-Mail als Spam markiert.
- **Deliveries (Zustellungen)**Delivery — Amazon SES hat die E-Mail erfolgreich an den E-Mail-Server des Empfängers übermittelt.
- **Opens (Öffnungsvorgänge)**Der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
- **Clicks (Klickvorgänge)**— Der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.
- **Rendering-Fehler**Rendering-Problems der Vorlage wurde aufgrund eines Rendering-Problems der Vorlage nicht gesendet. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail mit der API-Operation [SendTemplatedEmail](#) oder [SendBulkTemplatedEmail](#) senden. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen.
- **Verzögerungen durch Lieferungen**Delivery — 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.

Note

So fügen Sie die `DELIVERY_DELAY` dem -Ereignistyp einem Ereignisziel hinzuzufügen, müssen Sie den [UpdateConfigurationSetEventDestination](#) Der Vorgang in der Amazon SES API V2. Derzeit können Sie diesen Ereignistyp nicht mithilfe der Amazon SES S-Konsole einem Konfigurationssatz hinzufügen.

8. FürQuelle des WertesGeben Sie an, wie Amazon SES die Daten erhält, die es an CloudWatch weiterleitet. Die folgenden Quellen für Werte sind verfügbar:

- **Nachrichten-Tag**— Amazon SES ruft den Dimensionsnamen und den Wert aus einem Tag ab, der von Ihnen mittels eines `X-SES-Message-Tags`-Header oder `Tags`-API-Parameter. Weitere Informationen zur Verwendung von Nachrichten-Tags finden Sie unter [the section called "Schritt 3: Festlegen eines Konfigurationssatzes für den Versand"](#) (p. 323).

Note

Nachrichten-Tags können die Zahlen 0-9, die Buchstaben A-Z (Groß- und Kleinbuchstaben), Bindestriche (-) und Unterstriche (_) enthalten.

Sie können auch die `Nachrichten-Tag` Erstellen Sie Dimensionen basierend auf automatischen Amazon SES -Tags. 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 [Funktionsweise der -Ereignisveröffentlichung](#) (p. 313).

- **E-Mail-Header**Deliveries — 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 verwendet werden: `Received`, `To`, `From`, `DKIM-Signature`, `CC`, `message-id` oder `Return-Path`.

- **Verknüpfen mit**— 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?](#) (p. 551).
9. FürDimensions-NameGeben Sie den Namen der Dimension ein, die Sie an CloudWatch übergeben möchten. Geben Sie unter Default Value (Standardwert) den Wert der Dimension ein.

Note

Dimensionsnamen und Werte können nur die Buchstaben A bis Z, die Ziffern 0 bis 9, Unterstriche (_), at-Zeichen (@), Bindestriche (-) und Punkte (.) enthalten. Leerzeichen, Akzentbuchstaben, nicht-lateinische Zeichen und andere Sonderzeichen sind nicht zulässig.

10. Wenn Sie weitere Dimensionen hinzufügen möchten, wählen Sie Add Dimension (Dimension hinzufügen) aus. Wählen Sie andernfalls Speichern aus.

Auswählen von CloudWatch Dimensionen

Berücksichtigen Sie bei der Auswahl von Namen und Werten zur Verwendung als CloudWatch Dimensionen die folgenden Faktoren:

- Preis pro Metrik Sie können in CloudWatch grundlegende Amazon SES Metriken kostenlos anzeigen. Wenn Sie Metriken jedoch mithilfe der -Ereignisveröffentlichung sammeln, erstellen Sie benutzerdefinierte Metriken in CloudWatch. Jede eindeutige Kombination aus Ereignistyp, Dimensionsname und Dimensionswert erstellt in CloudWatch eine andere benutzerdefinierte Metrik. Wenn Sie CloudWatch verwenden, wird Ihnen jede von Ihnen erstellte benutzerdefinierte Metrik berechnet. 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 definieren, es sei denn, Sie sind sehr daran interessiert, Ihre E-Mail-Sendeereignisse nach „From“ (Von) -Domäne zu verfolgen. `ses:from-domain` weil es viele verschiedene Werte annehmen kann. Weitere Informationen hierzu finden Sie unter [Amazon CloudWatch – Preise](#).
- Metrikfilter Sofern eine Metrik über mehrere Dimensionen verfügt, können Sie nicht auf der Grundlage einzelner Dimensionen auf die Metrik in CloudWatch zugreifen. Aus diesem Grund sollten Sie sorgfältig überlegen, bevor Sie einem einzelnen CloudWatch Ereignisziel 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.
- Quelle des Dimensionswerts— 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 die Amazon SES Ereignisveröffentlichung 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 mit anderen Zeichen angeben, wird der Aufruf zum Senden von E-Mails weiterhin erfolgreich ausgeführt, die Ereignismetriken werden jedoch nicht an Amazon CloudWatch gesendet.

Weitere Informationen zu CloudWatch Konzepten finden Sie unter [Amazon CloudWatch Konzepte](#) im Amazon CloudWatch-Benutzerhandbuch.

Einrichten eines Kinesis Data Firehose Ereignisziels für die Veröffentlichung von Amazon SES Ereignissen

Ein Amazon Kinesis Data Firehose -Ereignisziel stellt eine Entität dar, die bestimmte E-Mail-Sendeereignisse von Amazon SES in Kinesis Data Firehose veröffentlicht. Da ein Kinesis Data Firehose Ereignisziel nur innerhalb eines Konfigurationssatzes vorhanden ist, müssen Sie zunächst [Erstellen eines Konfigurationssatzes](#) (p. 316). Als Nächstes fügen Sie dem Konfigurationssatz das Ereignisziel hinzu.

Dieser Abschnitt enthält ein Verfahren zum Erstellen eines Ereignisziels mithilfe der Amazon SES Konsole. Sie können auch die [UpdateConfigurationSetEventDestination](#)-Vorgang im Amazon SES API V2-Ziel von verwenden, um Ereignisziele zu erstellen und zu aktualisieren.

So fügen Sie ein Kinesis Data Firehose Ereignisziel zu einem Konfigurationssatz hinzu (Konsole)

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Amazon SES Konsole unter<https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.
3. Wählen Sie einen Konfigurationssatz aus der Liste der Konfigurationssätze aus. Wenn diese Liste leer ist, müssen Sie zuerst [einen Konfigurationssatz erstellen](#) (p. 316).
4. FürZiel hinzufügen, wählen SieWählen Sie einen ZieltypKlicken Sie auf und danach aufKinesis Data Firehose.
5. Geben Sie im Feld Name einen Namen für das Ereignisziel ein.
6. Wählen Sie für Event types mindestens einen Ereignistypen aus, der im Ereignisziel veröffentlicht werden soll:
 - Sends (Sendevorgänge)Send — der Anruf an Amazon SES war erfolgreich und Amazon SES wird versuchen, die E-Mail zu übermitteln.
 - Ablehnungen— Amazon SES hat die E-Mail zunächst akzeptiert, dann jedoch einen Virus darin erkannt und die E-Mail abgelehnt. Amazon SES hat nicht versucht, die E-Mail an den E-Mail-Server des Empfängers zu senden.
 - UnzustellbarkeitDer Mail-Server des Empfängers hat die E-Mail dauerhaft abgelehnt. Dieses Ereignis entspricht einer permanenten Unzustellbarkeit. Temporäre Unzustellbaritäten werden nur dann aufgenommen, wenn Amazon SES über einen bestimmten Zeitraum vergeblich versucht hat, die E-Mail zuzustellen.
 - Beschwerden— Die E-Mail wurde erfolgreich an den Empfänger zugestellt. Der Empfänger hat die E-Mail als Spam markiert.
 - Deliveries (Zustellungen)Delivery — Amazon SES hat die E-Mail erfolgreich an den E-Mail-Server des Empfängers übermittelt.
 - Opens (Öffnungsvorgänge)Der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
 - Clicks (Klickvorgänge)— Der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.
 - Rendering-FehlerRendering-Problems der Vorlage wurde aufgrund eines Rendering-Problems der Vorlage nicht gesendet. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail mit der API-Operation [SendTemplatedEmail](#) oder [SendBulkTemplatedEmail](#) senden. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen.
 - Verzögerungen durch LieferungenSend — 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.

Note

So fügen Sie die hinzuDELIVERY_DELAY-Ereignistyp an ein Ereignisziel übergeben, müssen Sie den[UpdateConfigurationSetEventDestination](#)Der Vorgang in der Amazon SES API V2. Derzeit können Sie diesen Ereignistyp nicht mithilfe der Amazon SES S-Konsole einem Konfigurationssatz hinzufügen.

7. Wählen Sie Enabled.
8. Für-Streameinen vorhandenen Kinesis Data Firehose Delivery-Stream aus oder wählen Sie unterErstellen eines neuen Streams, um mithilfe der Kinesis Data Firehose Konsole eine neue zu erstellen.

Weitere Informationen zum Erstellen eines Streams über die Kinesis Data Firehose Konsole finden Sie unter[Erstellen eines Amazon Kinesis Firehose Bereitstellungs-Streams](#)imEntwicklerhandbuch für Amazon Kinesis Data Firehose.

9. Für IAM-Rolle Wählen Sie für Amazon SES eine IAM-Rolle aus, für die zur Veröffentlichung in Kinesis Data Firehose in Ihrem Namen berechtigt ist. Sie können eine vorhandene Rolle auswählen, Amazon SES eine Rolle für Sie erstellen lassen oder Ihre eigene Rolle erstellen.

Wenn Sie eine vorhandene Rolle wählen oder eine eigene Rolle erstellen, müssen Sie die Richtlinien der Rolle manuell ändern, damit diese die Berechtigung erhält, auf den -Bereitstellungs-Stream zuzugreifen, und Amazon SES die Berechtigung erhält, diese Rolle zu übernehmen. Beispiele für Richtlinien finden Sie unter [Erteilen der Berechtigung zum Veröffentlichen in Ihrem Kinesis Data Firehose Delivery Stream an Amazon SES](#) (p. 321).

10. Wählen Sie Save (Speichern) aus.

Weitere Informationen zur Verwendung der `UpdateConfigurationSetEventDestinationAPI` zum Hinzufügen eines Kinesis Data Firehose Ereignisziels finden Sie in der [Amazon Simple Email Service API-Referenz](#).

[Erteilen der Berechtigung zum Veröffentlichen in Ihrem Kinesis Data Firehose Delivery Stream an Amazon SES](#)

Damit Amazon SES Datensätze in Ihrem Kinesis Data Firehose Zustellungsstream veröffentlichen kann, müssen Sie eine AWS Identity and Access Management (IAM) [Rolle](#) Die Berechtigungsrichtlinie und Vertrauensrichtlinie der Rolle anfügen oder ändern. Die Berechtigungsrichtlinie ermöglicht der Rolle, Datensätze in Ihrem Kinesis Data Firehose -Bereitstellungs-Stream zu veröffentlichen, und die Vertrauensrichtlinie ermöglicht Amazon SES, diese 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 befähigt die Rolle zur Veröffentlichung von Datensätzen in Ihrem Kinesis Data Firehose Bereitstellungs-Stream.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
        "firehose:PutRecordBatch"
      ],
      "Resource": [
        "arn:aws:firehose:REGION:ACCOUNT-ID:deliverystream/DELIVERY-STREAM-NAME "
      ]
    }
  ]
}
```

[Vertrauensrichtlinie](#)

Die folgende Vertrauensrichtlinie ermöglicht Amazon SES die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
```

```
    "Service": "ses.amazonaws.com"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "StringEquals": {
      "sts:ExternalId": "ACCOUNT-ID"
    }
  }
}
]
```

Einrichten eines -Amazon SNS Ereignisziels für die -Ereignisveröffentlichung

Ein Ereignisziel benachrichtigt Sie mithilfe von Amazon SNS über bestimmte E-Mail-Sendeereignisse. Da ein Amazon SNS Ereignisziel nur innerhalb eines Konfigurationssatzes vorhanden ist, müssen Sie [Erstellen eines Konfigurationssatzes \(p. 316\)](#) Vor dem Hinzufügen des -Ereignisziels zum Konfigurationssatz.

Dieser Abschnitt enthält ein Verfahren zum Erstellen eines Ereignisziels mithilfe der Amazon SES Konsole. Sie können auch die [UpdateConfigurationSetEventDestination](#)-Vorgang im Amazon SES API V2-Ziel von verwenden, um Ereignisziele zu erstellen und zu aktualisieren.

Note

Es ist auch möglich, Benachrichtigungen über Amazon SNS auf der Kontoebene zu erhalten. Das bedeutet, dass Sie jedes Mal eine Amazon SNS Benachrichtigung bekommen können, wenn in Ihrem gesamten Amazon SES S-Konto ein Sendeereignis eintritt. Wenn Sie anstelle von Benachrichtigungen auf Kontoebene die Ereignisveröffentlichung verwenden, können Sie Amazon SES so konfigurieren, dass Sie Benachrichtigungen nur zu bestimmten Ereignistypen oder nur für E-Mails erhalten, die mithilfe eines bestimmten Konfigurationssatzes gesendet werden. Weitere Informationen zum Einrichten von Amazon SNS Benachrichtigungen auf Kontoebene finden Sie unter [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen \(p. 288\)](#).

Für das Senden von Nachrichten an die Endpunkte, die für Ihre Amazon SNS -Themas abonniert sind, fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [Amazon SNS Preise](#).

So fügen Sie ein Amazon SNS Ereignisziel zu einem Konfigurationssatz hinzu

1. Wenn Sie dies nicht bereits getan haben, erstellen Sie ein Amazon SNS -Thema und abonnieren Sie es. Weitere Informationen finden Sie unter [Erste Schritte](#) im Amazon Simple Notification Service-Entwicklerhandbuch.
2. Öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
3. Wählen Sie im Navigationsbereich Configuration Sets aus.
4. Wählen Sie einen Konfigurationssatz aus der Liste der Konfigurationssätze aus. Wenn diese Liste leer ist, müssen Sie zuerst [einen Konfigurationssatz erstellen \(p. 316\)](#).
5. Wählen Sie unter Add Destination die Option Select a destination type und anschließend SNS aus.
6. Geben Sie im Feld Name einen Namen für das Ereignisziel ein.
7. Wählen Sie für Event types mindestens einen Ereignistypen aus, der im Ereignisziel veröffentlicht werden soll:
 - **Sends (Sendevorgänge)** Send — der Anruf an Amazon SES war erfolgreich und Amazon SES wird versuchen, die E-Mail zu übermitteln.
 - **Ablehnungen** — Amazon SES hat die E-Mail zunächst akzeptiert, dann jedoch einen Virus darin erkannt und die E-Mail abgelehnt. Amazon SES hat nicht versucht, die E-Mail an den E-Mail-Server des Empfängers zu senden.
 - **Unzustellbarkeit** Der Mail-Server des Empfängers hat die E-Mail dauerhaft abgelehnt. Dieses Ereignis entspricht einer permanenten Unzustellbarkeit. Temporäre Unzustellbaritäten werden nur

dann aufgenommen, wenn Amazon SES über einen bestimmten Zeitraum vergeblich versucht hat, die E-Mail zuzustellen.

- **Beschwerden**— Die E-Mail wurde erfolgreich an den Empfänger zugestellt. Der Empfänger hat die E-Mail als Spam markiert.
- **Deliveries (Zustellungen)**Delivery — Amazon SES hat die E-Mail erfolgreich an den E-Mail-Server des Empfängers übermittelt.
- **Opens (Öffnungsvorgänge)**Der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
- **Clicks (Klickvorgänge)**Click — Der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.
- **Rendering-Fehler**Rendering-Problems der Vorlage wurde aufgrund eines Rendering-Problems der Vorlage nicht gesendet. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail mit der API-Operation [SendTemplatedEmail](#) oder [SendBulkTemplatedEmail](#) senden. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen.
- **Verzögerungen durch Lieferungen**Send — 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.

Note

So fügen Sie die `DELIVERY_DELAY`-Ereignistyp an ein Ereignisziel übergeben, müssen Sie den [UpdateConfigurationSetEventDestination](#) Der Vorgang in der Amazon SES API V2. Derzeit können Sie diesen Ereignistyp nicht mithilfe der Amazon SES S-Konsole einem Konfigurationssatz hinzufügen.

8. Wählen Sie **Enabled**.
9. Für **Topic** Wählen Sie ein vorhandenes Amazon SNS -Thema aus oder wählen Sie **Erstellen eines neuen -Themas** Klicken Sie auf **+** um eine neue zu erstellen.

Weitere Informationen zum Erstellen eines Themas finden Sie unter [Erstellen eines Themas](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

10. Wählen Sie **Save (Speichern)** aus.
11. Weitere Informationen zum Verwenden eines Konfigurationssatzes für den Versand einer E-Mail finden Sie unter [Festlegen eines Konfigurationssatzes für das Senden von E-Mail](#) (p. 279).

Schritt 3: Festlegen eines Konfigurationssatzes für den Versand von E-Mail

Nach dem [Erstellen eines Konfigurationssatzes](#) (p. 316) und dem [Hinzufügen eines Ereignisziels](#) (p. 316) 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 Amazon SES-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
<code>SendEmail</code>	API-Parameter

Schnittstelle zum Senden von E-Mails	Möglichkeiten zum Veröffentlichen von Events
<code>SendRawEmail</code>	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.

- [Amazon SES API-Parameter verwenden \(p. 324\)](#)
- [Verwenden von Amazon SES-spezifischen E-Mail-Headern \(p. 324\)](#)
- [Verwenden von benutzerdefinierten E-Mail-Headern \(p. 325\)](#)

Darüber hinaus enthält dieses Handbuch mehrere Codebeispiele, die veranschaulichen, wie E-Mails mit Amazon SES programmgesteuert gesendet werden. Jedes dieser Codebeispiele enthält eine Methode zur Weitergabe eines Konfigurationssatzes beim Senden einer E-Mail. Weitere Informationen finden Sie unter [Amazon SES Codebeispiele \(p. 452\)](#).

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.

Amazon SES API-Parameter verwenden

Wenn Sie `SendEmail` oder `SendRawEmail` mit der Ereignisveröffentlichung verwenden möchten, geben Sie den Konfigurationssatz und die Nachrichten-Tags an, indem Sie Datenstrukturen mit dem Namen `ConfigurationSet` und `MessageTag` an den API-Aufruf weitergeben.

Weitere Informationen zur Verwendung der Amazon SES -API finden Sie unter [Amazon Simple Email Service API-Referenz](#).

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 mithilfe des Amazon SES-spezifischen Headers angeben. `X-SES-CONFIGURATION-SET` 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 Header-Namen oder -Werte für die Amazon SES -Ereignisveröffentlichung nicht im ASCII-Format angeben, wird der Aufruf zum Senden von E-Mails weiterhin erfolgreich ausgeführt, die Ereignismetriken werden jedoch nicht an Amazon CloudWatch ausgegeben.

Arbeiten mit Amazon SES Ereignisdaten

Nachdem Sie die [Ereignisveröffentlichung eingerichtet](#) (p. 315) 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 Konfigurationssatzes im Zusammenhang mit der E-Mail angegeben haben.

In diesem Abschnitt wird beschrieben, wie Sie Ihre E-Mail-Sendeereignisse von Amazon CloudWatch und Amazon Kinesis Data Firehose abrufen und wie Sie von Amazon SNS bereitgestellte Ereignisdaten interpretieren.

- [Abrufen von Amazon SES Ereignisdaten aus CloudWatch](#) (p. 325)
- [Abrufen von Amazon SES Ereignisdaten aus Kinesis Data Firehose](#) (p. 327)
- [Interpretieren von Amazon SES S-Ereignisdaten aus Amazon SNS](#) (p. 348)

Abrufen von Amazon SES Ereignisdaten aus CloudWatch

Amazon SES kann Metriken für Ihre E-Mail-Sendeereignisse an Amazon CloudWatch veröffentlichen. Wenn Sie Ereignisdaten in CloudWatch veröffentlichen, stellt es diese Metriken als einen geordneten Satz

an Zeitreihendaten bereit. Sie können diese Metriken verwenden, um die Leistung des E-Mail-Versands zu überwachen. Sie können beispielsweise die Beschwerdemetrik überwachen und einen CloudWatch Alarm festlegen, der ausgelöst wird, wenn die Metrik einen bestimmten Wert überschreitet.

Es gibt zwei Granularitätsstufen, in denen Amazon SES diese Ereignisse in CloudWatch veröffentlichen kann:

- In Ihrem AWS Konto Diese groben Metriken, die den Metriken entsprechen, die Sie mithilfe der Amazon SES Konsole und der `GetSendStatistics`-API sind Gesamtsummen für Ihr gesamtes AWS Konto. Amazon SES veröffentlicht diese Metriken automatisch in CloudWatch.
- Feinkörnig Diese Metriken werden anhand von E-Mail-Eigenschaften kategorisiert, die Sie mithilfe von Nachrichten-Tags. Um diese Metriken in CloudWatch zu veröffentlichen, müssen Sie [Einrichten der Ereignisveröffentlichung \(p. 315\)](#) mit einem CloudWatch Ereignisziel und [Festlegen eines Konfigurationssatzes \(p. 323\)](#) Wenn Sie eine E-Mail senden. Sie können auch Nachrichten-Tags angeben oder [auto-tags \(p. 313\)](#), die Amazon SES automatisch zur Verfügung stellt.

In diesem Abschnitt werden die verfügbaren Metriken beschrieben und wie Sie in CloudWatch angezeigt werden.

Verfügbare Metriken

Sie können folgende Amazon SES E-Mail-Sendemetriken an CloudWatch senden:

- Sends (Sendevorgänge) Send — der Anruf an Amazon SES war erfolgreich und Amazon SES wird versuchen, die E-Mail zu übermitteln.
- Ablehnungen — Amazon SES hat die E-Mail zunächst akzeptiert, dann jedoch einen Virus darin erkannt und die E-Mail abgelehnt. Amazon SES hat nicht versucht, die E-Mail an den E-Mail-Server des Empfängers zu senden.
- Unzustellbarkeit Der Mail-Server des Empfängers hat die E-Mail dauerhaft abgelehnt. Dieses Ereignis entspricht einer permanenten Unzustellbarkeit. Temporäre Unzustellbaritäten werden nur dann aufgenommen, wenn Amazon SES über einen bestimmten Zeitraum vergeblich versucht hat, die E-Mail zuzustellen.
- Beschwerden — Die E-Mail wurde erfolgreich an den Empfänger zugestellt. Der Empfänger hat die E-Mail als Spam markiert.
- Deliveries (Zustellungen) Delivery — Amazon SES hat die E-Mail erfolgreich an den E-Mail-Server des Empfängers übermittelt.
- Opens (Öffnungsvorgänge) Der Empfänger hat die Nachricht erhalten und sie in einem E-Mail-Client geöffnet.
- Clicks (Klickvorgänge) Click — Der Empfänger hat auf mindestens einen Link in der E-Mail geklickt.
- Rendering-Fehler Rendering-Problems der Vorlage wurde aufgrund eines Rendering-Problems der Vorlage nicht gesendet. Dieser Ereignistyp tritt nur auf, wenn Sie eine E-Mail mit der API-Operation [SendTemplatedEmail](#) oder [SendBulkTemplatedEmail](#) senden. Dieser Ereignistyp kann auftreten, wenn Vorlagendaten fehlen oder die Vorlagenparameter nicht mit den Daten übereinstimmen.
- Verzögerungen durch Lieferungen Send — 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.

Note

So fügen Sie die `DELIVERY_DELAY`-Ereignistyp an ein Ereignisziel übergeben, müssen Sie den [UpdateConfigurationSetEventDestination](#) Der Vorgang in der Amazon SES API V2. Derzeit können Sie diesen Ereignistyp nicht mithilfe der Amazon SES S-Konsole einem Konfigurationssatz hinzufügen.

Verfügbare Dimensionen

CloudWatch verwendet die Dimensionsnamen, die Sie angeben, wenn Sie ein CloudWatch Ereignisziel zu einem Konfigurationssatz in Amazon SES hinzufügen. Weitere Informationen finden Sie unter [Einrichten eines -CloudWatch Ereignisziels für die -Ereignisveröffentlichung \(p. 316\)](#).

Anzeigen von Amazon SES Metriken in der CloudWatch Konsole

Im folgenden Verfahren wird beschrieben, wie Sie die Amazon SES Metriken für die Ereignisveröffentlichung mit der CloudWatch Konsole anzeigen.

So zeigen Sie Metriken mit der CloudWatch-Konsole an:

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die CloudWatch Konsole unter<https://console.aws.amazon.com/cloudwatch/>.
2. Ändern Sie, falls erforderlich, die Region. Wählen Sie auf der Navigationsleiste die Region aus, in der sich Ihre AWS-Ressourcen befinden. Weitere Informationen finden Sie unter [Regionen und Endpunkte von AWS](#).
3. Wählen Sie im Navigationsbereich Metrics aus.
4. Erweitern Sie im Bereich All metrics AWS Namespaces und wählen Sie anschließend SES.
5. Zum Anzeigen von Metriken in Ihren gesamten AWS Konten, die Amazon SES automatisch veröffentlicht, wählen SieKennzahlen zum Senden von Konten. So zeigen Sie feinkörnig an[Ereignisveröffentlichung -Metriken \(p. 313\)](#)Wählen Sie die Kombination von Dimensionen, die Sie angegeben haben, als Sie[Einrichten Ihres CloudWatch Ereignisziels \(p. 316\)](#).
6. Wählen Sie die Metrik, die Sie anzeigen möchten.

Das Diagramm zeigt die Metrik im Laufe der Zeit an.

So zeigen Sie Metriken mit der AWS-Befehlszeilenschnittstelle (CLI) an

- Geben Sie als Eingabeaufforderung den folgenden Befehl ein:

```
aws cloudwatch list-metrics --namespace "AWS/SES"
```

Abrufen von Amazon SES Ereignisdaten aus Kinesis Data Firehose

Amazon SES veröffentlicht E-Mail-Sendeereignisse für Kinesis Data Firehose als JSON-Datensätze. Anschließend veröffentlicht Kinesis Data Firehose die Datensätze für das AWS -Service-Ziel, das Sie beim Einrichten des Bereitstellungs-Streams in Kinesis Data Firehose ausgewählt haben. Weitere Informationen zum Einrichten des Kinesis Data Firehose Bereitstellungs-Streams finden Sie unter[Erstellt einen Kinesis Data Firehose Bereitstellungs-Stream](#).imEntwicklerhandbuch für Amazon Kinesis Data Firehose.

Beispiele zur Verwendung von Kinesis Data Firehose zur Veröffentlichung der E-Mail-Sendeereignisse in Amazon Redshift und Amazon Elasticsearch Service finden Sie unter[Tutorials \(p. 369\)](#).

Themen in diesem Abschnitt:

- [Inhalte der Ereignisdaten, die Amazon SES in Kinesis Data Firehose veröffentlicht \(p. 328\)](#)
- [Beispiele für Ereignisdaten, die Amazon SES in Kinesis Data Firehose veröffentlicht \(p. 338\)](#)

Inhalte der Ereignisdaten, die Amazon SES in Kinesis Data Firehose veröffentlicht

Amazon SES veröffentlicht E-Mail-Sendeereignisdatensätze für Amazon Kinesis Data Firehose im JSON-Format. Wenn Sie Ereignisse in Kinesis Data Firehose veröffentlichen, fügt Amazon SES nach jedem JSON-Datensatz ein Zeilenumbruchzeichen ein.

Das JSON-Objekt der obersten Ebene enthält eine `eventType`-Zeichenfolge, ein `mail`-Objekt und ein Objekt des Typs `Bounce`, `Complaint`, `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure` oder `DeliveryDelay` (je nach Ereignistyp).

Beispieldatensätze für all diese Benachrichtigungstypen finden Sie unter [Beispiele für Ereignisdaten, die Amazon SES in Kinesis Data Firehose veröffentlicht](#) (p. 338).

Themen in diesem Abschnitt

- [JSON-Objekt der obersten Ebene](#) (p. 328)
- [Mail-Objekt](#) (p. 329)
- [Bounce-Objekt](#) (p. 330)
- [Complaint-Objekt](#) (p. 333)
- [Delivery-Objekt](#) (p. 335)
- [Send-Objekt](#) (p. 335)
- [Reject-Objekt](#) (p. 335)
- [Open-Objekt](#) (p. 335)
- [Click-Objekt](#) (p. 336)
- [Rendering Failure-Objekt](#) (p. 336)
- [DeliveryDelay-Objekt](#) (p. 336)

JSON-Objekt der obersten Ebene

Das JSON-Objekt der obersten Ebene in einem E-Mail-Sendeereignisdatensatz enthält die folgenden Felder.

Feldname	Beschreibung
<code>eventType</code>	Eine Zeichenfolge, die die Art des Ereignisses angibt. Mögliche Werte: <code>Delivery</code> , <code>Send</code> , <code>Reject</code> , <code>Open</code> , <code>Click</code> , <code>Bounce</code> , <code>Complaint</code> , <code>Rendering Failure</code> oder <code>DeliveryDelay</code> .
<code>mail</code>	Ein JSON-Objekt, das Informationen über die E-Mail enthält, die das Ereignis hervorgerufen hat.
<code>bounce</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Bounce</code> eingestellt ist. Es enthält Informationen über die Unzustellbarkeit.
<code>complaint</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Complaint</code> eingestellt ist. Es enthält Informationen über die Beschwerde.
<code>delivery</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Delivery</code> eingestellt ist. Es enthält Informationen über die Zustellung.
<code>send</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Send</code> eingestellt ist.

Feldname	Beschreibung
<code>reject</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Reject</code> eingestellt ist. Es enthält Informationen über die Ablehnung.
<code>open</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Open</code> eingestellt ist. Es enthält Informationen über das offene Ereignis.
<code>click</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Click</code> eingestellt ist. Es enthält Informationen über das Klick-Ereignis.
<code>failure</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Rendering Failure</code> eingestellt ist. Es enthält Informationen über das Rendering-Fehlerereignis.
<code>deliveryDelay</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>DeliveryDelay</code> eingestellt ist. Es enthält Informationen zur verzögerten Zustellung einer E-Mail.

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	Beschreibung
<code>timestamp</code>	Datum und Zeitpunkt, zu denen die Nachricht gesendet wurde, im ISO8601-Format (JJJJ-MM-TTThh: mm: ss.sZ).
<code>messageId</code>	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 in der ursprünglichen E-Mail in den Feldern <code>headers</code> und <code>commonHeaders</code> des Objekts <code>mail</code>.
<code>source</code>	Die E-Mail-Adresse, von der die Nachricht gesendet wurde (die <code>Envelope-MAIL-FROM</code> -Adresse).
<code>sourceArn</code>	Der Amazon-Ressourcenname (ARN) der Identität, die zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt <code>sourceArn</code> den ARN der ID an, die – gemäß Autorisierung durch den Identitätseigentümer – vom stellvertretenden Sender zum Senden

Feldname	Beschreibung
	der E-Mail verwendet werden soll. Weitere Informationen zur Sendeautorisierung finden Sie unter Verwenden der Sendeautorisierung (p. 162) .
<code>sendingAccountId</code>	Die AWS-Konto-ID des Kontos, das zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt <code>sendingAccountId</code> die Konto-ID des stellvertretenden Senders an.
<code>destination</code>	Eine Liste der E-Mail-Adressen, an die die ursprüngliche E-Mail gesendet wurde.
<code>headersTruncated</code>	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 <code>true</code> und <code>false</code> .
<code>headers</code>	Eine Liste der ursprünglichen Header der E-Mail. Jeder Header in der Liste verfügt über die Felder <code>name</code> und <code>value</code>. Note Jede Nachrichten-ID innerhalb <code>desheaders</code> stammt von der ursprünglichen Nachricht, die Sie an Amazon SES übergeben haben. Die Nachrichten-ID, die Amazon SES der Nachricht zugewiesen hat, befindet sich im <code>FeldmessageId</code>-Feld des <code>mailEin</code> - Objekt.
<code>commonHeaders</code>	Eine Liste der ursprünglichen, häufig verwendeten Header der E-Mail. Jeder Header in der Liste verfügt über die Felder <code>name</code> und <code>value</code>. Note Jede Nachrichten-ID innerhalb <code>descommonHeaders</code> stammt von der ursprünglichen Nachricht, die Sie an Amazon SES übergeben haben. Die Nachrichten-ID, die Amazon SES der Nachricht zugewiesen hat, befindet sich im <code>FeldmessageId</code>-Feld des <code>mailEin</code> - Objekt.

Bounce-Objekt

Das JSON-Objekt, das die Informationen zu einem `Bounce`-Ereignis enthält, weist immer die folgenden Felder auf.

Feldname	Beschreibung
<code>bounceType</code>	Der Unzustellbarstyp, wie er von Amazon SES festgelegt wurde.

Feldname	Beschreibung
<code>bounceSubType</code>	Der untergeordnete Typ der Unzustellbarkeit, wie er von Amazon SES festgelegt wurde.
<code>bouncedRecipients</code>	Eine Liste mit Informationen über die Empfänger der ursprünglichen E-Mail, an die diese nicht zugestellt werden konnte.
<code>timestamp</code>	Das Datum und der Zeitpunkt im ISO8601-Format (JJJJ-MM-TTThh:mm:ss.sZ), zu dem der ISP die Unzustellbarkeitsbenachrichtigung gesendet hat.
<code>feedbackId</code>	Eine eindeutige ID für die Unzustellbarkeit.
<code>reportingMTA</code>	Der Wert des <code>Reporting-MTA</code>-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	Beschreibung
<code>emailAddress</code>	Die E-Mail-Adresse des Empfängers. Ist eine DSN verfügbar, ist dies der Wert des <code>Final-Recipient</code> -Felds der DSN.

Wurde eine DSN an eine Unzustellbarkeitsbenachrichtigung angehängt, sind möglicherweise folgende Felder ebenfalls vorhanden.

Feldname	Beschreibung
<code>action</code>	Der Wert des <code>Action</code> -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.
<code>status</code>	Der Wert des <code>Status</code> -Felds der DSN. Dies ist der vom Transport unabhängige Statuscode pro

Feldname	Beschreibung
	Empfänger, der den Zustellstatus der Nachricht anzeigt.
<code>diagnosticCode</code>	Der vom berichtenden MTA gemeldete Statuscode. Dies ist der Wert des <code>Diagnostic-Code</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 Unzustellbaritäten und permanente Unzustellbarkeitsmeldungen, die nicht mehr von Amazon SES abgerufen werden. Wenn Sie erhalten Bounces markiert `Permanent` Die entsprechenden E-Mail-Adressen sollten Sie aus Ihrer Mailingliste entfernen; Sie werden in Zukunft nicht mehr an sie senden können. `Transient`-Bounces werden an Sie gesendet, wenn eine Nachricht mehrmals zeitweilig 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.

<code>bounceType</code>	<code>bounceSubType</code>	Beschreibung
<code>Undetermined</code>	<code>Undetermined</code>	konnte keinen bestimmten Grund für das Amazon SES inkten der Zustellung finden.
<code>Permanent</code>	<code>General</code>	Amazon SES hat eine allgemeine Unzustellbarkeitsbenachrichtigung erhalten. Wenn Sie diese Art von Unzustellbarkeit erhalten, sollten Sie die E-Mail-Adresse des Empfängers aus Ihrer Mailing-Liste entfernen.
<code>Permanent</code>	<code>NoEmail</code>	Amazon SES hat eine Benachrichtigung über eine permanente Unzustellbarkeit erhalten, 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.
<code>Permanent</code>	<code>Suppressed</code>	Amazon SES hat das Senden an diese Adresse unterdrückt, da bereits mehrere Zustellversuche aufgrund einer ungültigen Adresse fehlgeschlagen sind. Informationen zum Entfernen einer Adresse aus der Unterdrückungsliste finden Sie unter Verwenden der globalen Unterdrückungsliste von Amazon SES (p. 210) .
<code>Permanent</code>	<code>OnAccountSuppressionList</code>	Das Senden an diese Adresse hat Amazon SES unterdrückt, da sie sich auf der Seite befindet. Unterdrückungsliste auf Kontoebene (p. 201) .
<code>Transient</code>	<code>General</code>	Amazon SES hat eine allgemeine Unzustellbarkeitsbenachrichtigung erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger zukünftig möglich.

bounceType	bounceSubType	Beschreibung
Transient	MailboxFull	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung erhalten, da das Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger zukünftig möglich.
Transient	MessageTooLarge	Amazon SES hat eine Unzustellbarmachung aufgrund einer zu großen E-Mail erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie die Größe der Nachricht reduzieren.
Transient	ContentRejected	hat eine Unzustellbarmachung aufgrund eines abgelehnten Inhalts erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie den Inhalt der Nachricht ändern.
Transient	AttachmentRejected	hat eine Unzustellbarmachung 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	Beschreibung
<code>complainedRecipients</code>	Eine Liste mit Informationen zu Empfängern, die sich möglicherweise beschwert haben.
<code>timestamp</code>	Das Datum und der Zeitpunkt im ISO8601-Format (JJJJ-MM-TTThh:mm:ss.sZ), zu dem der ISP die Beschwerdebenachrichtigung gesendet hat.
<code>feedbackId</code>	Eine eindeutige ID für die Beschwerde.
<code>complaintSubType</code>	Der untergeordnete Typ der Beschwerde, wie er von Amazon SES festgelegt wurde.

Ist zudem ein Feedback-Bericht an die Beschwerde angehängt, sind möglicherweise die folgenden Felder vorhanden.

Feldname	Beschreibung
<code>userAgent</code>	Der Wert des <code>User-Agent</code> -Felds aus dem Feedback-Bericht. Gibt den Namen und die Version des Systems an, das den Bericht generiert hat.
<code>complaintFeedbackType</code>	Der Wert des <code>Feedback-Type</code> -Felds aus dem Feedback-Bericht, der vom ISP empfangen wurde. Enthält die Art des Feedbacks.

Feldname	Beschreibung
<code>arrivalDate</code>	Der Wert des <code>Arrival-Date</code> -Felds oder des <code>Received-Date</code> -Felds aus dem Feedback-Bericht im ISO8601-Format (JJJJ-MM-TTThh:mm:ss.sZ). Dieses Feld ist möglicherweise 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 sich beschwert hat, in der Benachrichtigung über eine Beschwerde nicht offenlegen, enthält diese Liste Informationen zu Empfängern, die sich möglicherweise beschwert haben. Dabei basiert die Einschätzung auf den Empfängern der ursprünglichen E-Mail und dem ISP, der die Beschwerde an uns übermittelt hat. Amazon SES führt einen Abgleich mit der ursprünglichen Nachricht durch, um diese Empfängerliste festzulegen.

JSON-Objekte in dieser Liste enthalten das folgende Feld.

Feldname	Beschreibung
<code>emailAddress</code>	Die E-Mail-Adresse des Empfängers.

Beschwerdetypen

Sie sehen möglicherweise die folgenden Beschwerdetypen im `complaintFeedbackType`-Feld, so wie sie vom meldenden ISP entsprechend der [Internet Assigned Numbers Authority-Website](#) zugewiesen wurden:

Feldname	Beschreibung
<code>abuse</code>	Weist auf unerwünschte E-Mails oder eine andere Art von E-Mail-Missbrauch hin.
<code>auth-failure</code>	Bericht über einen E-Mail-Authentifizierungsfehler.
<code>fraud</code>	Weist auf einen Betrug oder Phishing hin.
<code>not-spam</code>	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.
<code>other</code>	Gibt eine andere Art von Feedback an, das nicht zu den registrierten Typen passt.
<code>virus</code>	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	Beschreibung
<code>timestamp</code>	Das Datum und die Zeit, zu der Amazon SES die E-Mail an den Mailserver des Empfängers übermittelt hat, angezeigt im ISO8601-Format (JJJ-MM-TTthh:mm:ss.sz) enthalten.
<code>processingTimeMillis</code>	Die Zeit in Millisekunden zwischen dem Zeitpunkt, als Amazon SES die Anforderung des Absenders angenommen hat, und dem Zeitpunkt, als Amazon SES die Nachricht an den Mail-Server des Empfängers übergeben hat.
<code>recipients</code>	Eine Liste der beabsichtigten Empfänger, für die das Übermittlungsereignis gilt.
<code>smtpResponse</code>	Die SMTP-Antwort des Remote-ISP, der die E-Mail von Amazon SES zugelassen hat. Diese Nachricht variiert je nach E-Mail, empfangendem Mail-Server und empfangendem ISP.
<code>reportingMTA</code>	Der Hostname des Amazon SES Mail-Servers, der die E-Mail gesendet 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	Beschreibung
<code>reason</code>	Der Grund für die Ablehnung der E-Mail. Der einzige mögliche Wert ist <code>Bad content</code> . Dies 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 zuzustellen.

Open-Objekt

Das JSON-Objekt, das die Informationen zu einem `Open`-Ereignis enthält, enthält immer die folgenden Felder.

Feldname	Beschreibung
<code>ipAddress</code>	Die IP-Adresse des Empfängers.

Feldname	Beschreibung
timestamp	Datum und Zeitpunkt, zu denen das Open-Ereignis eintrat, im ISO8601-Format (JJJJ-MM-TTThh: mm:ss.sZ).
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	Beschreibung
ipAddress	Die IP-Adresse des Empfängers.
timestamp	Datum und Zeitpunkt, zu denen das Klick-Ereignis eintrat, im ISO8601-Format (JJJJ-MM-TTThh: mm:ss.sZ).
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 <code>ses:tags</code> -Attributs hinzugefügt wurden. Weitere Informationen zum Hinzufügen von Tags zu Links in Ihren E-Mail finden Sie unter F5. Kann ich Links mit eindeutigen Bezeichnern markieren? (p. 551) in den Häufig gestellte Fragen zu -E-Mail-Sendemetriken (p. 549).

Rendering Failure-Objekt

Das JSON-Objekt enthält Informationen über ein `Rendering Failure`-Ereignis mit den folgenden Feldern.

Feldname	Beschreibung
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	Beschreibung
<code>delayType</code>	Die Art der Verzögerung. Die möglichen Werte sind: • InternalFailure— Ein internes Amazon SES Problem führte dazu, dass die Nachricht verzögert wurde. • Allgemeines— Ein generischer Fehler ist während der SMTP-Konversation aufgetreten. • MailboxFull— Das Postfach des Empfängers ist voll und kann keine zusätzlichen Nachrichten empfangen. • SpamDetected— Der E-Mail-Server des Empfängers hat eine große Menge unerwünschter E-Mails von Ihrem Konto erkannt. • RecipientServerError— Ein temporäres Problem mit dem E-Mail-Server des Empfängers verhindert die Zustellung der Nachricht. • IPFailure— Die IP-Adresse, die die Nachricht sendet, wird vom E-Mail-Anbieter des Empfängers blockiert oder gedrosselt. • TransientCommunicationGeneral— Es ist ein vorübergehender Kommunikationsfehler während der SMTP-Konversation mit dem E-Mail-Anbieter des Empfängers aufgetreten. • byoipHostNameLookupNicht verfügbar— Amazon SES konnte den DNS-Hostnamen für Ihre IP-Adressen nicht nachschlagen. Diese Art von Verzögerung tritt nur auf, wenn Sie Bring Your Own IP (p. 197) verwenden. • Unbestimmt— Amazon SES konnte den Grund für die Lieferverzögerung nicht ermitteln.
<code>delayedRecipients</code>	Ein Objekt, das Informationen zum E-Mail-Empfänger enthält
<code>expirationTime</code>	Das Datum und die Uhrzeit, zu der Amazon SES die Zustellung der Nachricht nicht mehr versucht. Dieser Wert wird im ISO 8601-Format angezeigt.
<code>reportingMTA</code>	Die IP-Adresse des Message Transfer Agent (MTA), der die Verzögerung gemeldet hat
<code>timestamp</code>	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	Beschreibung
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

Beispiele für Ereignisdaten, die Amazon SES in Kinesis Data Firehose veröffentlicht

In diesem Abschnitt finden Sie Beispiele für die Typen von E-Mail-Versandereignisdatensätzen, die Amazon SES in Kinesis Data Firehose veröffentlicht.

Themen in diesem Abschnitt:

- [Bounce-Datensatz \(p. 338\)](#)
- [Complaint-Datensatz \(p. 339\)](#)
- [Delivery-Datensatz \(p. 341\)](#)
- [Send-Datensatz \(p. 342\)](#)
- [Reject-Datensatz \(p. 343\)](#)
- [Open-Datensatz \(p. 344\)](#)
- [Click-Datensatz \(p. 346\)](#)
- [Rendering Failure-Datensatz \(p. 347\)](#)
- [DeliveryDelay-Datensatz \(p. 348\)](#)

Bounce-Datensatz

Es folgt ein Beispiel für ein Bounce-Ereignisdatensatz, den Amazon SES in Kinesis Data 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

Es folgt ein Beispiel für ein Complaint-Ereignisdatensatz, den Amazon SES in Kinesis Data 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

Es folgt ein Beispiel für einDelivery-Ereignisdatensatz, den Amazon SES in Kinesis Data 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",
    "reportingMTA": "mta.example.com"
  }
}
```

Send-Datensatz

Es folgt ein Beispiel für einSend-Ereignisdatensatz, den Amazon SES in Kinesis Data 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

Es folgt ein Beispiel für einReject-Ereignisdatensatz, den Amazon SES in Kinesis Data 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

Es folgt ein Beispiel für einen Open-Ereignisdatensatz, den Amazon SES in Kinesis Data 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": [
    "ses-user"
  ],
  "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

Es folgt ein Beispiel für ein Click-Ereignisdatensatz, den Amazon SES in Kinesis Data 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

Es folgt ein Beispiel für ein `Rendering Failure`-Ereignisdatensatz, den Amazon SES in Kinesis Data 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-Datensatz

Es folgt ein Beispiel für einDeliveryDelay-Ereignisdatensatz, den Amazon SES in Kinesis Data 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"
    }]
  }
}
```

Interpretieren von Amazon SES S-Ereignisdaten aus Amazon SNS

Amazon SES veröffentlicht E-Mail-Versandereignisse an Amazon Simple Notification Service (Amazon SNS) als JSON-Datensätze. Anschließend stellt Amazon SNS Benachrichtigungen an die Endpunkte zu, die das Amazon SNS -Thema im Zusammenhang mit dem Ereignisziel abonniert haben. Weitere Informationen zum Einrichten von Themen und Abonnements in Amazon SNS finden Sie unter [Erste Schritte](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

Eine Beschreibung der Datensatzinhalte und Beispieldatensätze finden Sie in den folgenden Abschnitten.

- [Inhalte von Ereignisdatensätzen \(p. 349\)](#)
- [Beispiele für Ereignisdatensätze \(p. 359\)](#)

Inhalt der Ereignisdaten, die Amazon SES in Amazon SNS veröffentlicht

Amazon SES veröffentlicht E-Mail-Sendeereignisdatensätze für Amazon Simple Notification Service im JSON-Format.

Das JSON-Objekt der obersten Ebene enthält eine `eventType`-Zeichenfolge, ein `mail`-Objekt und ein Objekt des Typs `Bounce`, `Complaint`, `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure` oder `DeliveryDelay` (je nach Ereignistyp).

Beispieldatensätze für all diese Benachrichtigungstypen finden Sie unter [Beispiele für Ereignisdaten, die Amazon SES in Amazon SNS veröffentlicht](#) (p. 359).

Themen in diesem Abschnitt:

- [JSON-Objekt der obersten Ebene](#) (p. 349)
- [Mail-Objekt](#) (p. 350)
- [Bounce-Objekt](#) (p. 351)
- [Complaint-Objekt](#) (p. 354)
- [Delivery-Objekt](#) (p. 356)
- [Send-Objekt](#) (p. 356)
- [Reject-Objekt](#) (p. 356)
- [Open-Objekt](#) (p. 356)
- [Click-Objekt](#) (p. 357)
- [Rendering Failure-Objekt](#) (p. 357)
- [DeliveryDelay-Objekt](#) (p. 357)

JSON-Objekt der obersten Ebene

Das JSON-Objekt der obersten Ebene in einem E-Mail-Sendeereignisdatensatz enthält die folgenden Felder.

Feldname	Beschreibung
<code>eventType</code>	Eine Zeichenfolge, die die Art des Ereignisses angibt. Mögliche Werte: <code>Delivery</code> , <code>Send</code> , <code>Reject</code> , <code>Open</code> , <code>Click</code> , <code>Bounce</code> , <code>Complaint</code> , <code>Rendering Failure</code> oder <code>DeliveryDelay</code> .
<code>mail</code>	Ein JSON-Objekt, das Informationen über die E-Mail enthält, die das Ereignis hervorgerufen hat.
<code>bounce</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Bounce</code> eingestellt ist. Es enthält Informationen über die Unzustellbarkeit.
<code>complaint</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Complaint</code> eingestellt ist. Es enthält Informationen über die Beschwerde.
<code>delivery</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Delivery</code> eingestellt ist. Es enthält Informationen über die Zustellung.
<code>send</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Send</code> eingestellt ist.

Feldname	Beschreibung
<code>reject</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Reject</code> eingestellt ist. Es enthält Informationen über die Ablehnung.
<code>open</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Open</code> eingestellt ist. Es enthält Informationen über das offene Ereignis.
<code>click</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Click</code> eingestellt ist. Es enthält Informationen über das Klick-Ereignis.
<code>failure</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>Rendering Failure</code> eingestellt ist. Es enthält Informationen über das Rendering-Fehlerereignis.
<code>deliveryDelay</code>	Dieses Feld ist nur vorhanden, wenn <code>eventType</code> auf <code>DeliveryDelay</code> eingestellt ist. Es enthält Informationen zur verzögerten Zustellung einer E-Mail.

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	Beschreibung
<code>timestamp</code>	Datum und Zeitpunkt, zu denen die Nachricht gesendet wurde, im ISO8601-Format (JJJJ-MM-TTThh:mm:ss.Z).
<code>messageId</code>	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 in der ursprünglichen E-Mail in den Feldern <code>headers</code> und <code>commonHeaders</code> des Objekts <code>mail</code>.
<code>source</code>	Die E-Mail-Adresse, von der die Nachricht gesendet wurde (die <code>Envelope-MAIL-FROM</code> -Adresse).
<code>sourceArn</code>	Der Amazon-Ressourcenname (ARN) der Identität, die zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt <code>sourceArn</code> den ARN der ID an, die – gemäß Autorisierung durch den Identitätseigentümer – vom stellvertretenden Sender zum Senden

Feldname	Beschreibung
	der E-Mail verwendet werden soll. Weitere Informationen zur Sendeautorisierung finden Sie unter Verwenden der Sendeautorisierung (p. 162) .
<code>sendingAccountId</code>	Die AWS-Konto-ID des Kontos, das zum Senden der E-Mail verwendet wurde. Im Fall einer Sendeautorisierung gibt <code>sendingAccountId</code> die Konto-ID des stellvertretenden Senders an.
<code>destination</code>	Eine Liste der E-Mail-Adressen, an die die ursprüngliche E-Mail gesendet wurde.
<code>headersTruncated</code>	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 <code>true</code> und <code>false</code> .
<code>headers</code>	Eine Liste der ursprünglichen Header der E-Mail. Jeder Header in der Liste verfügt über die Felder <code>name</code> und <code>value</code>. Note Jede Nachrichten-ID innerhalb <code>desheaders</code> stammt von der ursprünglichen Nachricht, die Sie an Amazon SES übergeben haben. Die Nachrichten-ID, die Amazon SES der Nachricht zugewiesen hat, befindet sich im <code>FeldmessageId</code>-Feld des <code>mailEin</code> - Objekt.
<code>commonHeaders</code>	Eine Liste der ursprünglichen, häufig verwendeten Header der E-Mail. Jeder Header in der Liste verfügt über die Felder <code>name</code> und <code>value</code>. Note Jede Nachrichten-ID innerhalb <code>descommonHeaders</code> stammt von der ursprünglichen Nachricht, die Sie an Amazon SES übergeben haben. Die Nachrichten-ID, die Amazon SES der Nachricht zugewiesen hat, befindet sich im <code>FeldmessageId</code>-Feld des <code>mailEin</code> - Objekt.

Bounce-Objekt

Das JSON-Objekt enthält Informationen über ein Bounce-Ereignis mit den folgenden Feldern.

Feldname	Beschreibung
<code>bounceType</code>	Der Unzustellbarstyp, wie er von Amazon SES festgelegt wurde.

Feldname	Beschreibung
<code>bounceSubType</code>	Der untergeordnete Typ der Unzustellbarkeit, wie er von Amazon SES festgelegt wurde.
<code>bouncedRecipients</code>	Eine Liste mit Informationen über die Empfänger der ursprünglichen E-Mail, an die diese nicht zugestellt werden konnte.
<code>timestamp</code>	Das Datum und der Zeitpunkt im ISO8601-Format (JJJJ-MM-TTThh:mm:ss.sZ), zu dem der ISP die Unzustellbarkeitsbenachrichtigung gesendet hat.
<code>feedbackId</code>	Eine eindeutige ID für die Unzustellbarkeit.
<code>reportingMTA</code>	Der Wert des <code>Reporting-MTA</code>-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	Beschreibung
<code>emailAddress</code>	Die E-Mail-Adresse des Empfängers. Ist eine DSN verfügbar, ist dies der Wert des <code>Final-Recipient</code> -Felds der DSN.

Wurde eine DSN an eine Unzustellbarkeitsbenachrichtigung angehängt, sind möglicherweise folgende Felder ebenfalls vorhanden.

Feldname	Beschreibung
<code>action</code>	Der Wert des <code>Action</code> -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.
<code>status</code>	Der Wert des <code>Status</code> -Felds der DSN. Dies ist der vom Transport unabhängige Statuscode pro

Feldname	Beschreibung
	Empfänger, der den Zustellstatus der Nachricht anzeigt.
<code>diagnosticCode</code>	Der vom berichtenden MTA gemeldete Statuscode. Dies ist der Wert des <code>Diagnostic-Code</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 Unzustellbaritäten und permanente Unzustellbarkeitsmeldungen, die nicht mehr von Amazon SES abgerufen werden. Wenn Sie erhalten Bounces markiert `Permanent` Die entsprechenden E-Mail-Adressen sollten Sie aus Ihrer Mailingliste entfernen; Sie werden in Zukunft nicht mehr an sie senden können. `Transient`-Bounces werden an Sie gesendet, wenn eine Nachricht mehrmals zeitweilig 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.

<code>bounceType</code>	<code>bounceSubType</code>	Beschreibung
<code>Undetermined</code>	<code>Undetermined</code>	konnte keinen bestimmten Grund für das Amazon SES inkten der Zustellung finden.
<code>Permanent</code>	<code>General</code>	Amazon SES hat eine allgemeine Unzustellbarkeitsbenachrichtigung erhalten. Wenn Sie diese Art von Unzustellbarkeit erhalten, sollten Sie die E-Mail-Adresse des Empfängers aus Ihrer Mailing-Liste entfernen.
<code>Permanent</code>	<code>NoEmail</code>	Amazon SES hat eine Benachrichtigung über eine permanente Unzustellbarkeit erhalten, 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.
<code>Permanent</code>	<code>Suppressed</code>	Amazon SES hat das Senden an diese Adresse unterdrückt, da bereits mehrere Zustellversuche aufgrund einer ungültigen Adresse fehlgeschlagen sind. Informationen zum Entfernen einer Adresse aus der Unterdrückungsliste finden Sie unter Verwenden der globalen Unterdrückungsliste von Amazon SES (p. 210) .
<code>Permanent</code>	<code>OnAccountSuppressionList</code>	Das Senden an diese Adresse hat Amazon SES unterdrückt, da sie sich auf der Seite befindet. Unterdrückungsliste auf Kontoebene (p. 201) .
<code>Transient</code>	<code>General</code>	Amazon SES hat eine allgemeine Unzustellbarkeitsbenachrichtigung erhalten.

bounceType	bounceSubType	Beschreibung
		Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger zukünftig möglich.
Transient	MailboxFull	Amazon SES hat eine Unzustellbarkeitsbenachrichtigung erhalten, da das Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger zukünftig möglich.
Transient	MessageTooLarge	Amazon SES hat eine Unzustellbarmachung aufgrund einer zu großen E-Mail erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie die Größe der Nachricht reduzieren.
Transient	ContentRejected	hat eine Unzustellbarmachung aufgrund eines abgelehnten Inhalts erhalten. Möglicherweise ist eine erfolgreiche Zustellung an diesen Empfänger möglich, wenn Sie den Inhalt der Nachricht ändern.
Transient	AttachmentRejected	hat eine Unzustellbarmachung 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	Beschreibung
<code>complainedRecipients</code>	Eine Liste mit Informationen zu Empfängern, die sich möglicherweise beschwert haben.
<code>timestamp</code>	Das Datum und der Zeitpunkt im ISO8601-Format (JJJJ-MM-TTThh:mm:ss.sZ), zu dem der ISP die Beschwerdebenachrichtigung gesendet hat.
<code>feedbackId</code>	Eine eindeutige ID für die Beschwerde.
<code>complaintSubType</code>	Der untergeordnete Typ der Beschwerde, wie er von Amazon SES festgelegt wurde.

Ist zudem ein Feedback-Bericht an die Beschwerde angehängt, sind möglicherweise die folgenden Felder vorhanden.

Feldname	Beschreibung
<code>userAgent</code>	Der Wert des <code>User-Agent</code> -Felds aus dem Feedback-Bericht. Gibt den Namen und die Version des Systems an, das den Bericht generiert hat.

Feldname	Beschreibung
<code>complaintFeedbackType</code>	Der Wert des <code>Feedback-Type</code> -Felds aus dem Feedback-Bericht, der vom ISP empfangen wurde. Enthält die Art des Feedbacks.
<code>arrivalDate</code>	Der Wert des <code>Arrival-Date</code> -Felds oder des <code>Received-Date</code> -Felds aus dem Feedback-Bericht im ISO8601-Format (JJJJ-MM-TTThh:mm:ss.sZ). Dieses Feld ist möglicherweise 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

Die meisten Internetdienstanbieter machen die E-Mail-Adressen von Empfängern unkenntlich, die Beschwerden einreichen. 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	Beschreibung
<code>emailAddress</code>	Die E-Mail-Adresse des Empfängers.

Beschwerdetypen

Sie sehen möglicherweise die folgenden Beschwerdetypen im `complaintFeedbackType`-Feld, so wie sie vom meldenden ISP entsprechend der [Internet Assigned Numbers Authority-Website](#) zugewiesen wurden:

Feldname	Beschreibung
<code>abuse</code>	Weist auf unerwünschte E-Mails oder eine andere Art von E-Mail-Missbrauch hin.
<code>auth-failure</code>	Bericht über einen E-Mail-Authentifizierungsfehler.
<code>fraud</code>	Weist auf einen Betrug oder Phishing hin.
<code>not-spam</code>	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.
<code>other</code>	Gibt eine andere Art von Feedback an, das nicht zu den registrierten Typen passt.
<code>virus</code>	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` hat, Amazon SES die Nachricht zunächst akzeptiert, aber nicht versucht, sie zu senden, da sie sich auf der [Unterdrückungsliste auf Kontoebene](#) (p. 201).

Delivery-Objekt

Das JSON-Objekt enthält Informationen über ein `Delivery`-Ereignis mit den folgenden Feldern.

Feldname	Beschreibung
<code>timestamp</code>	Das Datum und die Zeit, zu der Amazon SES die E-Mail an den Mailserver des Empfängers übermittelt hat, angezeigt im ISO8601-Format (JJJ-MM-TTthh:mm:ss.sz) enthalten.
<code>processingTimeMillis</code>	Die Zeit in Millisekunden zwischen dem Zeitpunkt, als Amazon SES die Anforderung des Absenders angenommen hat, und dem Zeitpunkt, als Amazon SES die Nachricht an den Mail-Server des Empfängers übergeben hat.
<code>recipients</code>	Eine Liste der beabsichtigten Empfänger, für die das Übermittlungsereignis gilt.
<code>smtpResponse</code>	Die SMTP-Antwort des Remote-ISP, der die E-Mail von Amazon SES zugelassen hat. Diese Nachricht variiert je nach E-Mail, empfangendem Mail-Server und empfangendem ISP.
<code>reportingMTA</code>	Der Hostname des Amazon SES Mail-Servers, der die E-Mail gesendet 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	Beschreibung
<code>reason</code>	Der Grund für die Ablehnung der E-Mail. Der einzige mögliche Wert ist <code>bad_content</code> . Dies 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 zuzustellen.

Open-Objekt

Das JSON-Objekt enthält Informationen über ein `Open`-Ereignis mit den folgenden Feldern.

Feldname	Beschreibung
<code>ipAddress</code>	Die IP-Adresse des Empfängers.
<code>timestamp</code>	Datum und Zeitpunkt, zu denen das Open-Ereignis eintrat, im ISO8601-Format (JJJJ-MM-TTThh: mm:ss.sZ).
<code>userAgent</code>	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	Beschreibung
<code>ipAddress</code>	Die IP-Adresse des Empfängers.
<code>timestamp</code>	Datum und Zeitpunkt, zu denen das Klick-Ereignis eintrat, im ISO8601-Format (JJJJ-MM-TTThh: mm:ss.sZ).
<code>userAgent</code>	Der Benutzeragent des Clients, den der Empfänger zum Klicken auf einen Link in der E-Mail verwendet hat.
<code>link</code>	Die URL des Links, auf den der Empfänger geklickt hat.
<code>linkTags</code>	Eine Liste der Tags, die dem Link mithilfe des <code>ses:tags</code> -Attributs hinzugefügt wurden. Weitere Informationen zum Hinzufügen von Tags zu Links in Ihren E-Mail finden Sie unter F5. Kann ich Links mit eindeutigen Bezeichnern markieren? (p. 551) in den Häufig gestellte Fragen zu -E-Mail-Sendemetriken (p. 549).

Rendering Failure-Objekt

Das JSON-Objekt enthält Informationen über ein `Rendering Failure`-Ereignis mit den folgenden Feldern.

Feldname	Beschreibung
<code>templateName</code>	Der Name der Vorlage, die zum Senden der E-Mail verwendet wurde.
<code>errorMessage</code>	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	Beschreibung
<code>delayType</code>	Die Art der Verzögerung. Die möglichen Werte sind: • InternalFailure— Ein internes Amazon SES Problem führte dazu, dass die Nachricht verzögert wurde. • Allgemeines— Ein generischer Fehler ist während der SMTP-Konversation aufgetreten. • MailboxFull— Das Postfach des Empfängers ist voll und kann keine zusätzlichen Nachrichten empfangen. • SpamDetected— Der E-Mail-Server des Empfängers hat eine große Menge unerwünschter E-Mails von Ihrem Konto erkannt. • RecipientServerError— Ein temporäres Problem mit dem E-Mail-Server des Empfängers verhindert die Zustellung der Nachricht. • IPFailure— Die IP-Adresse, die die Nachricht sendet, wird vom E-Mail-Anbieter des Empfängers blockiert oder gedrosselt. • TransientCommunicationGeneral— Es ist ein vorübergehender Kommunikationsfehler während der SMTP-Konversation mit dem E-Mail-Anbieter des Empfängers aufgetreten. • byoipHostNameLookupNicht verfügbar— Amazon SES konnte den DNS-Hostnamen für Ihre IP-Adressen nicht nachschlagen. Diese Art von Verzögerung tritt nur auf, wenn Sie Bring Your Own IP (p. 197) verwenden. • Unbestimmt— Amazon SES konnte den Grund für die Lieferverzögerung nicht ermitteln.
<code>delayedRecipients</code>	Ein Objekt, das Informationen zum E-Mail-Empfänger enthält
<code>expirationTime</code>	Das Datum und die Uhrzeit, zu der Amazon SES die Zustellung der Nachricht nicht mehr versucht. Dieser Wert wird im ISO 8601-Format angezeigt.
<code>reportingMTA</code>	Die IP-Adresse des Message Transfer Agent (MTA), der die Verzögerung gemeldet hat
<code>timestamp</code>	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	Beschreibung
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

Beispiele für Ereignisdaten, die Amazon SES in Amazon SNS veröffentlicht

In diesem Abschnitt finden Sie Beispiele für die Typen von E-Mail-Sendeereignisdatensätzen, die Amazon SES bei Amazon SNS veröffentlicht.

Themen in diesem Abschnitt:

- [Bounce-Datensatz](#) (p. 359)
- [Complaint-Datensatz](#) (p. 360)
- [Delivery-Datensatz](#) (p. 362)
- [Send-Datensatz](#) (p. 363)
- [Reject-Datensatz](#) (p. 364)
- [Open-Datensatz](#) (p. 365)
- [Click-Datensatz](#) (p. 367)
- [Rendering Failure-Datensatz](#) (p. 368)
- [DeliveryDelay-Datensatz](#) (p. 369)

Bounce-Datensatz

Es folgt ein Beispiel für einBounce-Ereignisdatensatz, den Amazon SES in 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

Es folgt ein Beispiel für ein Complaint-Ereignisdatensatz, den Amazon SES in 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

Es folgt ein Beispiel für einDelivery-Ereignisdatensatz, den Amazon SES in 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",
  "reportingMTA": "mta.example.com"
}
}
```

Send-Datensatz

Es folgt ein Beispiel für ein Send-Ereignisdatensatz, den Amazon SES in Amazon SNS 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

Es folgt ein Beispiel für einReject-Ereignisdatensatz, den Amazon SES in 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

Es folgt ein Beispiel für einen Open-Ereignisdatensatz, den Amazon SES in 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": [
      "ses-user"
    ],
    "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

Es folgt ein Beispiel für einClick-Ereignisdatensatz, den Amazon SES in 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": "text/html; charset=UTF-8"  
      }  
    ]  
  }  
}
```

```
    "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

Es folgt ein Beispiel für einen Rendering Failure-Ereignisdatensatz, den Amazon SES in 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-Datensatz

Es folgt ein Beispiel für einen DeliveryDelay-Ereignisdatensatz, den Amazon SES in 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"
      }
    ]
  }
}
```

Ereignisveröffentlichung – Tutorials

In diesem Abschnitt werden Tutorials beschrieben, wie Sie die Amazon SES -Ereignisveröffentlichung mit AWS -Services zum Analysieren und Visualisieren Ihrer Daten verwenden können.

Themen in diesem Abschnitt:

- [Analysieren von E-Mail-Sendeereignissen mit Amazon Redshift \(p. 369\)](#)
- [Darstellen von E-Mail-Sendeereignissen in Amazon CloudWatch \(p. 382\)](#)
- [Analysieren von E-Mail-Sendeereignissen mit Amazon Kinesis Data Analytics \(p. 385\)](#)

Analysieren von E-Mail-Sendeereignissen mit Amazon Redshift

In diesem Tutorial veröffentlichen Sie E-Mail-Sendeereignisse von Amazon SES in einem Amazon Kinesis Data Firehose -Bereitstellungs-Stream, der die Daten an Amazon Redshift übermittelt. Anschließend stellen Sie eine Verbindung zur Amazon Redshift -Datenbank her und nutzen ein SQL-Abfragetool, um aus der Datenbank die E-Mail-Sendeereignisse von Amazon SES abzufragen, die bestimmte Kriterien erfüllen.

In den folgenden Abschnitten finden Sie eine schrittweise Anleitung für dieses Verfahren.

- [Voraussetzungen \(p. 370\)](#)
- [Schritt 1: Erstellen eines Amazon Redshift Clusters \(p. 370\)](#)
- [Schritt 2: Connect Sie sich mit Ihrem Amazon Redshift Cluster \(p. 371\)](#)
- [Schritt 3: Erstellen einer Datenbank-Tabelle \(p. 374\)](#)

- [Schritt 4: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream. \(p. 376\)](#)
- [Schritt 5: Einrichten eines Konfigurationssatzes \(p. 379\)](#)
- [Schritt 6: Versenden von E-Mails \(p. 380\)](#)
- [Schritt 7: E-Mail-Sendeereignissen \(p. 381\)](#)

Prerequisites

Für dieses Tutorial benötigen Sie Folgendes:

- Ein AWS-Konto Um auf alle von AWS bereitgestellten Webservices zuzugreifen, müssen Sie zunächst unter ein AWS-Konto erstellen <https://aws.amazon.com/>.
- bestätigte E-Mail-Adresse Verifizierte E-Mail-Adresse (Absender) oder Domäne, um E-Mails mit Amazon SES senden zu können, müssen Sie den Besitz ihrer E-Mail-Adresse (Absender) oder Domäne nachweisen. Falls Sie sich in einer Sandbox-Umgebung befinden, müssen auch die Empfängeradressen verifiziert werden. Sie können E-Mail-Adressen oder ganze Domänen verifizieren, jedoch ist in diesem Tutorial nur die Bestätigung einer E-Mail-Adresse erforderlich, damit Sie eine E-Mail über die Amazon SES Konsole versenden können (das ist die einfachste Möglichkeit, eine E-Mail zu senden). Weitere Informationen zum Verifizieren einer E-Mail-Adresse finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
- Ein SQL-Abfragefööl— Amazon Redshift stellt weder SQL-Clienttools noch -Bibliotheken bereit oder installiert diese. Daher müssen Sie selbst ein Tool für den Zugriff auf die Amazon Redshift Cluster, die Ihre Amazon SES Ereignisse enthalten, installieren. In diesem Tutorial wird dafür [SQL Workbench/J](#) verwendet, ein kostenloses plattformübergreifendes SQL-Abfragetool, das nicht von einem bestimmten DBMS abhängig ist. Dieser Abschnitt enthält Verfahren zur Installation von SQL Workbench/J.

So installieren Sie SQL Workbench/J

1. Lesen Sie die [Softwarelizenz zu SQL Workbench/J](#).
2. Laden Sie sich auf der [SQL Workbench/J-Website](#) das entsprechende Paket für Ihr Betriebssystem herunter.
3. Rufen Sie die Seite [Installing and starting SQL Workbench/J](#) auf und installieren Sie SQL Workbench/J.

Important

Beachten Sie die JRE-Versionsvorgabe für SQL Workbench/J und vergewissern Sie sich, dass Sie die richtige Version verwenden. Andernfalls kann die Client-Anwendung nicht ausgeführt werden.

4. Wechseln Sie zu [Konfigurieren einer JDBC-Verbindung](#) Laden Sie einen Amazon Redshift JDBC-Treiber für herunter, damit SQL Workbench/J eine Verbindung zum Cluster herstellen kann.

Nächster Schritt

[Schritt 1: Erstellen eines Amazon Redshift Clusters \(p. 370\)](#)

Schritt 1: Erstellen eines Amazon Redshift Clusters

Um einen Amazon Redshift Cluster zu erstellen, gehen Sie zum [Amazon Redshift Konsole](#) und wählen Sie **Cluster starten**. Ein Assistent führt Sie durch die Optionsauswahl für den Cluster und bietet Standardwerte für die meisten Optionen an.

In diesem einfachen Tutorial geben Sie einen Cluster-Namen und ein Passwort an. Bei allen anderen Optionen übernehmen Sie die Standardwerte. Es ist nicht erforderlich, spezifische Werte für die Amazon SES Ereignisveröffentlichung einzugeben.

Important

Der Cluster, den Sie in diesem Tutorial bereitstellen, wird in einer Live-Umgebung ausgeführt. Solange dieser ausgeführt wird, fallen Gebühren für Ihr AWS-Konto an. Um unnötige Kosten zu vermeiden, sollten Sie den Cluster löschen, wenn Sie damit fertig sind. Weitere Informationen zu Preisen finden Sie in der [Amazon Redshift Preisseite](#).

Nächster Schritt

[Schritt 2: Connect Sie sich mit Ihrem Amazon Redshift Cluster \(p. 371\)](#)

Schritt 2: Connect Sie sich mit Ihrem Amazon Redshift Cluster

Nun stellen Sie mithilfe eines SQL-Clienttools eine Verbindung zum Cluster her. In diesem Tutorial verwenden Sie den SQL Workbench/J-Client, den Sie bereits im Abschnitt [Voraussetzungen \(p. 370\)](#) installiert haben.

Führen Sie die folgenden Schritte aus, um diesen Abschnitt abzuschließen:

- [Abrufen der Verbindungszeichenfolge \(p. 371\)](#)
- [Herstellen einer Verbindung zwischen SQL Workbench/J und Cluster \(p. 372\)](#)

Abrufen der Verbindungszeichenfolge

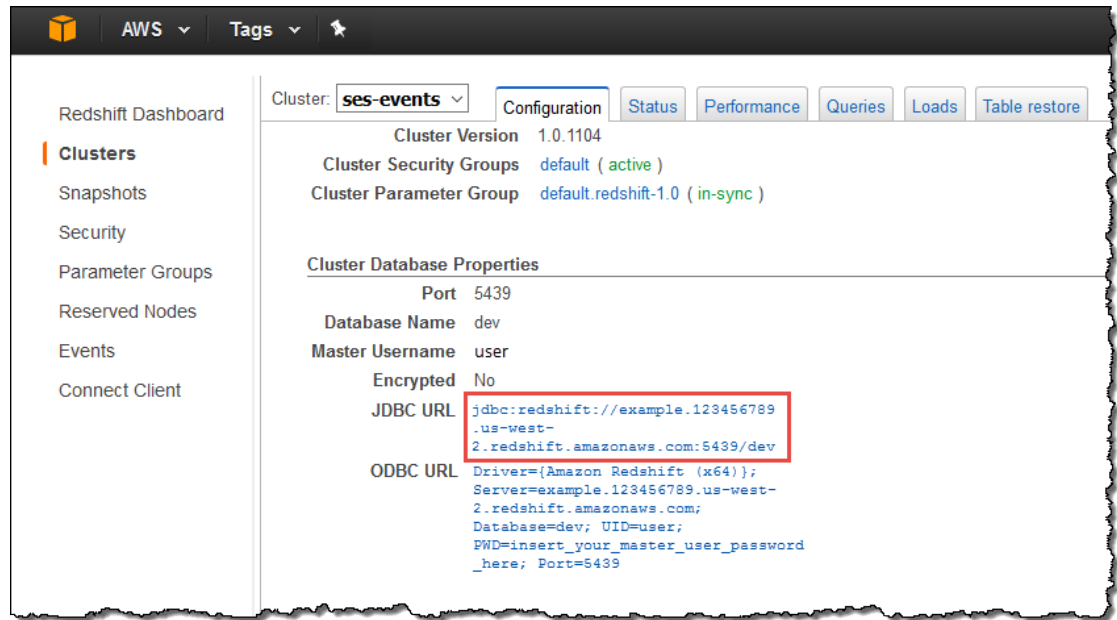
Im folgenden Verfahren wird beschrieben, wie Sie die Verbindungszeichenfolge abrufen, mit der Sie die Verbindung von SQL Workbench/J zum Amazon Redshift -Cluster herstellen.

So rufen Sie die Verbindungszeichenfolge ab

1. Wählen Sie im Navigationsbereich der Amazon Redshift Konsole aus-Cluster.
2. Zum Öffnen des Clusters wählen Sie Ihren Cluster-Namen aus.
3. Kopieren Sie auf der Registerkarte Configuration (Konfiguration) unter Cluster Database Properties (Eigenschaften der Cluster-Datenbank) den JDBC-URL des Clusters.

Note

Der Endpunkt des Clusters ist erst verfügbar, wenn der Cluster erstellt wurde und verfügbar ist.

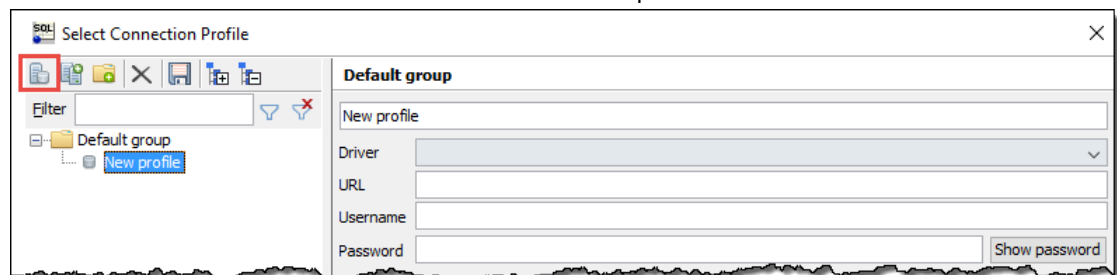


Herstellen einer Verbindung zwischen SQL Workbench/J und Cluster

Im folgenden Verfahren wird beschrieben, wie Sie eine Verbindung von SQL Workbench/J zum Cluster herstellen. Hierbei wird vorausgesetzt, dass Sie SQL Workbench/J wie unter [Prerequisites \(p. 370\)](#) beschrieben auf dem Computer installiert haben.

So stellen Sie die Verbindung zwischen SQL Workbench/J und Cluster her

1. Öffnen Sie SQL Workbench/J.
2. Wählen Sie File und anschließend Connect window aus.
3. Klicken Sie auf die Schaltfläche Create a new connection profile.



4. Geben Sie im Feld New profile einen Namen für das Profil ein.
5. Klicken Sie unten links im Fenster auf Manage Drivers.
6. Klicken Sie im Dialogfeld Manage Drivers auf Create a new entry und fügen Sie die Treiber wie folgt hinzu.



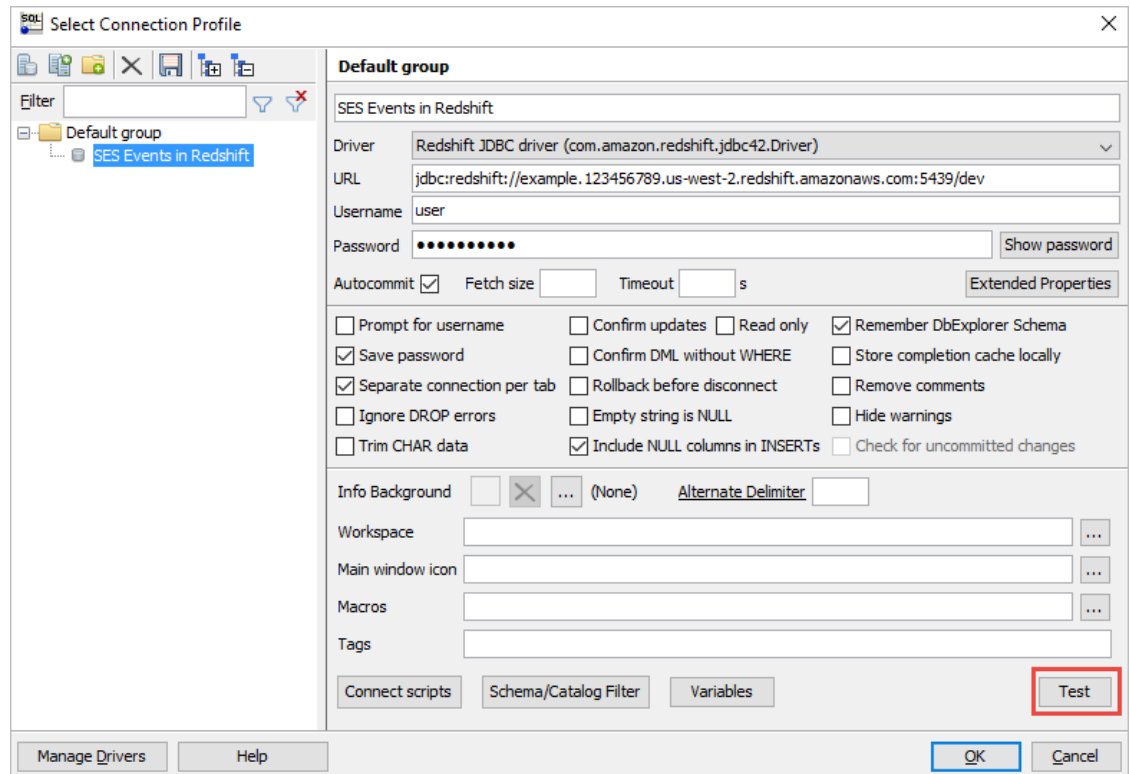
- a. Geben Sie im Feld Name den Namen des Treibers ein.
- b. Klicken Sie neben Library auf das Ordnersymbol.
- c. Navigieren Sie zum Speicherort des Treibers (den Sie im Thema [Konfigurieren einer JDBC-Verbindung](#) heruntergeladen haben), wählen Sie den Treiber aus und klicken Sie auf Open (Öffnen).
- d. Klicken Sie auf OK.

Sie werden zum Dialogfeld Select Connection Profile zurückgeleitet.

7. Wählen Sie im Feld Driver den soeben hinzugefügten Treiber aus.
8. FürURLFügen Sie im Feld [Amazon Redshift Konsole](#).
9. FürBenutzername:den Benutzernamen ein, den Sie im Thema [Einrichten des Amazon Redshift Clusters \(p. 370\)](#).
10. FürPasswortGeben Sie das Passwort ein, das Sie beim Erstellen des Amazon Redshift-Clusters verwendet haben.
11. Wählen Sie Autocommit aus.
12. Wählen Sie zum Testen der Verbindung Test aus.

Note

Sollte bei diesem Verbindungsversuch ein Timeout auftreten, muss ggf. die IP-Adresse zu der Sicherheitsgruppe hinzugefügt werden, die eingehenden Datenverkehr von IP-Adressen zulässt. Weitere Informationen finden Sie unter [Verbindung wird zurückgewiesen oder schlägt fehl](#) im Amazon Redshift Datenbankentwicklerhandbuch.



13. Klicken Sie oben in der Menüleiste auf die Schaltfläche Save profile list.

14. Klicken Sie auf OK.

SQL Workbench/J stellt die Verbindung zum Amazon Redshift Cluster her.

Nächster Schritt

[Schritt 3: Erstellen einer Datenbank-Tabelle \(p. 374\)](#)

Schritt 3: Erstellen einer Datenbank-Tabelle

Nachdem Sie die Verbindung zur initialen Datenbank in Amazon Redshift hergestellt haben, sollten Sie diese als Basis verwenden, um eine neue Datenbank zu erstellen. In diesem einfachen Tutorial wird eine Tabelle erstellt, damit die Daten der Veröffentlichung der Amazon SES Ereignisveröffentlichung direkt in der initialen Datenbank bleiben.

In diesem Tutorial wird davon ausgegangen, dass die folgenden Felder in den [Datensätzen der E-Mail-Sendeereignisse \(p. 328\)](#) interessant sind. Alle diese Felder mit Ausnahme von `mail.tags.campaign`, werden automatisch von Amazon SES bereitgestellt. Das Feld `mail.tags.campaign` wird unter [Schritt 6: Versenden von E-Mails \(p. 380\)](#) beim Versenden einer E-Mail mit `campaign` als Nachrichten-Tag beschrieben.

- `mail.messageId`
- `eventType`
- `mail.sendingAccountId`
- `mail.timestamp`
- `mail.destination`
- `mail.tags.ses:configuration-set`

- mail.tags.campaign

Für den Zugriff auf diese Informationen in der Datenbank ist eine Tabelle erforderlich. Im folgenden Verfahren wird beschrieben, wie Sie diese Informationen beim Erstellen der Tabelle in der Datenbank angeben.

Note

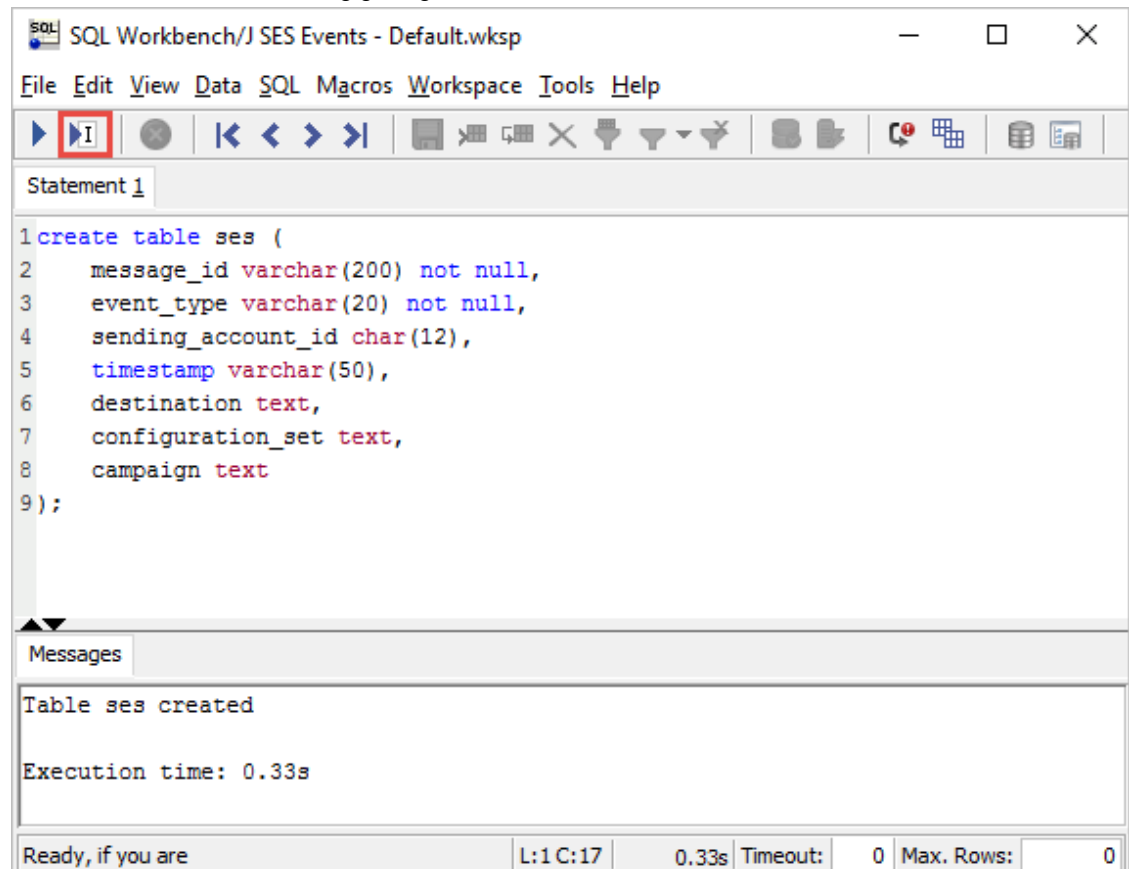
Es wird davon ausgegangen, dass SQL Workbench/J auf dem Computer ausgeführt wird und mit dem Amazon Redshift -Cluster verbunden ist, wie unter beschrieben [vorheriger Schritt \(p. 371\)](#).

So erstellen Sie eine Tabelle mit SQL Workbench/J

1. Kopieren Sie in SQL Workbench/J folgenden Code und fügen Sie ihn im Fenster Statement 1 ein.

```
create table ses (  
    message_id varchar(200) not null,  
    event_type varchar(20) not null,  
    sending_account_id char(12),  
    timestamp varchar(50),  
    destination text,  
    configuration_set text,  
    campaign text  
);
```

2. Platzieren Sie den Cursor in der Anweisung (vor dem Semikolon) und klicken Sie auf Execute current statement, wie in der Abbildung gezeigt.



3. Überprüfen Sie im Bereich Messages, ob die Tabelle erfolgreich erstellt wurde.

Nächster Schritt

[Schritt 4: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream. \(p. 376\)](#)

Schritt 4: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream.

Um E-Mail-Versandereignisse an Amazon Kinesis Data Firehose veröffentlichen zu können, müssen Sie einen Kinesis Data Firehose-Bereitstellungs-Stream erstellen. Beim Einrichten des Kinesis Data Firehose Bereitstellungs-Streams wählen Sie aus, wo Kinesis Data Firehose die Daten veröffentlicht. In diesem Tutorial wird Kinesis Data Firehose so konfiguriert, dass die Daten in Amazon Redshift veröffentlicht werden. Als Zwischenschritt soll Kinesis Data Firehose die Datensätze in Amazon S3 veröffentlichen. Dabei müssen Sie angeben, wie Amazon Redshift Datensätze aus Amazon S3 in die Tabelle kopiert, die im Verzeichnis erstellt wurde [vorheriger Schritt \(p. 374\)](#).

In diesem Abschnitt wird gezeigt, wie Sie einen Kinesis Data Firehose Bereitstellungs-Stream erstellen, der Daten an Amazon Redshift sendet. Zudem erfahren Sie, wie Sie den Bereitstellungs-Stream bearbeiten und angeben, auf welche Weise Amazon Redshift die Daten der Amazon SES Ereignisveröffentlichung in Amazon S3 kopieren soll.

Note

Sie müssen bereits [Einrichten des Amazon Redshift Clusters \(p. 370\)](#), [verbunden mit Ihrem Cluster \(p. 371\)](#), und [Erstellen einer Datenbank-Tabelle \(p. 374\)](#), wie bereits vorangehende Schritte erläutert.

Erstellt einen Kinesis Data Firehose Bereitstellungs-Stream.

Im folgenden Verfahren wird beschrieben, wie Sie einen Kinesis Data Firehose -Bereitstellungs-Stream erstellen, der Daten in Amazon Redshift veröffentlicht und Amazon S3 als zwischengeschalteten Speicherort verwendet.

So erstellen Sie einen Lieferdatenstrom von Kinesis Data Firehose zu Amazon Redshift

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Kinesis Data Firehose Konsole unter <https://console.aws.amazon.com/firehose/>.
2. Wählen Sie Create Delivery Stream aus.
3. Wählen Sie auf der Seite Destination die folgenden Optionen aus.
 - Zielbereich— Wählen Sie Amazon Redshift aus.
 - Delivery stream name – Geben Sie einen Namen für den Bereitstellungs-Stream an.
 - S3 bucket – Wählen Sie New S3 bucket aus, geben Sie einen Bucket-Namen ein, wählen Sie eine Region aus und klicken Sie auf Create Bucket.
 - Redshift-ClusterWählen Sie den Amazon Redshift Cluster aus, den Sie in einem vorigen Schritt erstellt haben.
 - Redshift database – Geben Sie dev an (das ist der Standardname für eine Datenbank).
 - Redshift table – Geben Sie mit ses die unter [Schritt 3: Erstellen einer Datenbank-Tabelle \(p. 374\)](#) erstellte Tabelle an.
 - Redshift table columns – Dieses Feld bleibt leer.
 - Redshift Benutzername— Geben Sie den Benutzernamen ein, den Sie im Thema [Einrichten des Amazon Redshift Clusters \(p. 370\)](#).
 - Redshift KennwortGeben Sie das Passwort ein, das Sie beim Erstellen des Amazon Redshift-Clusters verwendet haben.
 - Redshift COPY options – Dieses Feld bleibt leer.
 - Retry duration – Übernehmen Sie den Standardwert.

- Befehl COPY— Übernehmen Sie den Standardwert. Dieses Feld aktualisieren Sie im nächsten Verfahren.
4. Wählen Sie Next.
 5. Übernehmen Sie auf der Seite Configuration für dieses einfache Tutorial die Standardeinstellungen der Felder. Sie müssen hier nur eine IAM-Rolle auswählen, um Kinesis Data Firehose den Zugriff auf Ihre Ressourcen zu gewähren, wie im folgenden Verfahren beschrieben.
 - a. Wählen Sie im Feld IAM Role die Option Select an IAM role aus.
 - b. Wählen Sie im Dropdown-Menü unter Create/Update existing IAM role den Eintrag Firehose delivery IAM role aus.

Sie werden zur IAM-Konsole umgeleitet.

- c. Übernehmen Sie in der IAM-Konsole die Standardeinstellungen der Felder und klicken Sie auf der IAM-Konsole auf **Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf.**

The screenshot shows the AWS IAM console interface. At the top, there's a header with the AWS logo, 'AWS' dropdown, 'Tags' dropdown, and a star icon. Below this, a message states: 'Amazon Kinesis Firehose is requesting permission to use resources in your account'. A sub-message says: 'Click Allow to give Amazon Kinesis Firehose Read and Write access to resources in your account.' There's a 'Hide Details' link. Below that, the 'Role Summary' section is visible, showing 'Role: Provides access to AWS Services and Resources', 'Description', 'IAM Role: firehose_delivery_role', and 'Policy Name: Create a new Role Policy'. There's a 'View Policy Document' link. At the bottom right, there are two buttons: 'Don't Allow' and 'Allow'. The 'Allow' button is highlighted with a red rectangular box.

Sie kehren zu den Einrichtungsschritten für Kinesis Data Firehose in der Kinesis Data Firehose-Konsole zurück.

6. Wählen Sie Next.
7. Prüfen Sie auf der Seite Review Ihre Einstellungen und wählen Sie Create Delivery Stream aus.

Amazon Redshift Kopieroptionen festlegen

Als Nächstes müssen Sie Amazon Redshift angeben, wie Sie die JSON-Datensätze der Amazon SES Ereignisveröffentlichung in die unter erstellte Datenbanktabelle kopieren möchten. [Schritt 3: Erstellen einer Datenbank-Tabelle \(p. 374\)](#). Dazu bearbeiten Sie die Kopieroptionen im Kinesis Data Firehose Bereitstellungs-Stream.

Für diesen Schritt wird eine JSONPaths-Datei benötigt. Eine JSONPaths-Datei ist eine Textdatei, in der für den Amazon Redshift COPY-Befehl festgelegt wird, auf welche Weise die JSON-Quelldaten geparkt werden sollen. In diesem Verfahren wird eine JSONPaths-Datei zur Verfügung gestellt. Weitere

Informationen zu JSONPaths-Dateien finden Sie unter [COPY aus JSON-Format](#) im Amazon Redshift Datenbankentwicklerhandbuch.

Sie laden die JSONPaths-Datei in den Amazon S3 Bucket hoch, den Sie beim Erstellen des Kinesis Data Firehose -Bereitstellungs-Streams eingerichtet haben. Dann ändern Sie die COPY-Optionen des Kinesis Data Firehose -Bereitstellungs-Streams, damit die hochgeladene JSONPaths-Datei verwendet wird. Diese Schritte werden im folgenden Verfahren beschrieben.

So legen Sie die Amazon Redshift COPY-Befehlsoptionen fest

1. Erstellen einer JSONPaths-Datei— Erstellen Sie auf Ihrem Computer eine Datei mit dem Namen `jsonpaths.json`. Kopieren Sie folgenden Text und fügen Sie ihn in die Datei ein. Speichern Sie anschließend die Datei.

```
{
  "jsonpaths": [
    "$.mail.messageId",
    "$.eventType",
    "$.mail.sendingAccountId",
    "$.mail.timestamp",
    "$.mail.destination",
    "$.mail.tags.ses:configuration-set",
    "$.mail.tags.campaign"
  ]
}
```

2. Laden Sie die JSONPaths-Datei in den Amazon S3 Bucket hoch.— Rufen Sie auf [Amazon S3-Konsole](#) und laden Sie die Datei in den Bucket hoch, den Sie beim Einrichten des Kinesis Data Firehose Bereitstellungs-Streams unter [Erstellt einen Kinesis Data Firehose Bereitstellungs-Stream](#) (p. 376).
3. Legen Sie den Befehl COPY in den Kinesis Data Firehose Bereitstellungs-Stream fest Sie haben nun alle Informationen und können die Syntax des COPY-Befehls festlegen, mit dem Amazon Redshift die Daten in die von Ihnen erstellte Tabelle überträgt. Im folgenden Verfahren wird beschrieben, wie Sie die COPY-Befehlsinformationen in den Einstellungen des Kinesis Data Firehose -Bereitstellungs-Streams aktualisieren.
 1. Rufen Sie auf [Kinesis Data Firehose](#).
 2. **UNDER**Bereitstellungsstreams von Redshift Wählen Sie den Bereitstellungs-Stream für Kinesis Data Firehose aus, den Sie für die Amazon SES Ereignisveröffentlichung erstellt haben.
 3. Klicken Sie auf der Seite Details auf Edit.
 4. Geben Sie im Feld Redshift COPY options den folgenden Text ein und ersetzen Sie dabei die folgenden Werte durch Ihre eigenen:
 - S3-BUCKET-NAME— Der Name des Amazon S3 Buckets, in dem Kinesis Data Firehose Ihre Daten ablegt, auf die Amazon Redshift zugegriffen werden kann. Diesen Bucket haben Sie beim Einrichten des Kinesis Data Firehose Bereitstellungs-Streams unter [Schritt 4: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream](#) (p. 376). Ein Beispiel ist `my-bucket`.
 - REGION— Die Region, in der sich Ihre Amazon SES, Kinesis Data Firehose, Amazon S3 und Amazon Redshift befinden. Ein Beispiel ist `us-west-2`.

```
json 's3://S3-BUCKET-NAME/jsonpaths.json' region 'REGION';
```

5. Wählen Sie Save (Speichern) aus.

Delivery Streams > ses-stream

Use the tabs below to view, edit and monitor your delivery stream.

Details Monitoring S3 Logs Redshift Logs Delete Delivery Stream

Cancel Save

Delivery stream name* ses-stream

S3 bucket* example-bucket

S3 prefix S3 Prefix

IAM role* firehose_delivery_role

S3 buffer size (MB)* 5

S3 buffer interval (sec)* 300

S3 Compression UNCOMPRESSED

S3 Encryption No Encryption

Status ACTIVE

Error logging ☒ Enable ☐ Disable

Redshift cluster* ses-events

Redshift database* dev

Redshift table* ses

Redshift table columns Redshift table columns

Redshift username* user

Redshift password* *****

Redshift COPY options json 's3://S3-BUCKET-NAME/jsonpaths.json' region 'REGION';

Retry duration (sec)* 3600

COPY command COPY ses FROM 's3://example-bucket/<manifest>' CREDENTIALS 'aws_access_key_id=<aws-access-key-id>; aws_secret_access_key=<aws-secret-access-key>' MANIFEST json 's3://S3-BUCKET-NAME/jsonpaths.json' region 'REGION';

Nächster Schritt

[Schritt 5: Einrichten eines Konfigurationssatzes \(p. 379\)](#)

Schritt 5: Einrichten eines Konfigurationssatzes

Um Amazon SES so einzurichten, dass die E-Mail-Sendeereignisse in Amazon Kinesis Data Firehose veröffentlicht werden, erstellen Sie zunächst einen Konfigurationssatz und fügen diesem dann ein Ereignisziel hinzu. In diesem Abschnitt werden die dafür erforderlichen Schritte beschrieben.

Sofern Sie bereits über einen Konfigurationssatz verfügen, können Sie das Kinesis Data Firehose-Ziel zu diesem hinzufügen. Fahren Sie in diesem Falle mit [Hinzufügen eines Kinesis Data Firehose Ereignisziels \(p. 379\)](#) fort.

Erstellen eines Konfigurationssatzes

Im folgenden Verfahren wird das Erstellen eines Konfigurationssatzes beschrieben.

So erstellen Sie einen Konfigurationssatz

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.
3. Wählen Sie im Inhaltsbereich Create Configuration Set aus.
4. Geben Sie einen Namen für den Konfigurationssatz ein und wählen Sie Create Configuration Set aus.
5. Klicken Sie auf Close.

Hinzufügen eines Kinesis Data Firehose Ereignisziels

Im folgenden Verfahren wird beschrieben, wie Sie ein Kinesis Data Firehose-Ereignisziel zum erstellten Konfigurationssatz hinzufügen.

So fügen Sie ein Kinesis Data Firehose Ereignisziel zum Konfigurationssatz hinzu

1. Wählen Sie den Konfigurationssatz aus der Liste der Konfigurationssätze aus.
2. Für Ziel hinzufügen, wählen Sie Wählen Sie einen Zieltyp Klicken Sie auf und danach auf Kinesis Data Firehose.
3. Geben Sie im Feld Name einen Namen für das Ereignisziel ein.
4. Wählen Sie alle Einträge unter Event types aus.
5. Wählen Sie Enabled.
6. Wählen Sie im Feld Stream den Bereitstellungs-Stream aus, den Sie unter [Schritt 4: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream. \(p. 376\)](#) erstellt haben.
7. Wählen Sie im Feld IAM role die Option Let SES make a new role aus und geben Sie dann einen Namen für die Rolle ein.
8. Wählen Sie Save (Speichern) aus.
9. Verwenden Sie die Zurück-Schaltfläche Ihres Browsers, um die Seite Edit Configuration Set zu verlassen.

Nächster Schritt

[Schritt 6: Versenden von E-Mails \(p. 380\)](#)

Schritt 6: Versenden von E-Mails

Damit Amazon SES E-Mail-bezogene Ereignisse veröffentlicht, müssen Sie beim Senden der E-Mail einen Konfigurationssatz angeben. Sie können auch Nachrichten-Tags zur Kategorisierung der E-Mail einbinden. In diesem Abschnitt wird beschrieben, wie Sie mithilfe der Amazon SES -Konsole eine einfache E-Mail senden, in der ein Konfigurationssatz und Nachrichten-Tags angegeben sind. Sie senden die E-Mail an den Amazon SES Postfachsimulator, damit Sie Unzustellbarkeits-, Beschwerde- und andere E-Mail-Sendeergebnisse testen können.

So senden Sie eine E-Mail mit der Amazon SES Konsole

1. Melden Sie sich beim an. AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Klicken Sie im Navigationsbereich der Amazon SES Konsole unter Identitätsmanagement, wählen Sie E-Mail-Adressen.
3. Markieren Sie in der Liste der Identitäten eine E-Mail-Adresse, die erfolgreich für Sie [Bestätigt mit Amazon SES \(p. 52\)](#).
4. Wählen Sie Send a Test Email aus.
5. Wählen Sie im Dialogfeld Send Test Email im Feld Email Format die Option Raw aus.
6. Für die Bis-Adresse eine Adresse aus dem Feld [Amazon SES Postfach-Simulator \(p. 198\)](#), wie beispielsweise `complaint@simulator.amazonses.com` oder `bounce@simulator.amazonses.com`.
7. Kopieren Sie die gesamte folgende Nachricht und fügen Sie diese in das Textfeld Message (Nachricht) ein. Ersetzen Sie dabei `CONFIGURATION-SET-NAME` durch den Namen des Konfigurationssatzes, den Sie unter [Schritt 5: Einrichten eines Konfigurationssatzes \(p. 379\)](#) erstellt haben, und ersetzen Sie `FROM-ADDRESS` durch die verifizierte Adresse, von der Sie diese E-Mail senden.

```
X-SES-MESSAGE-TAGS: campaign=book
X-SES-CONFIGURATION-SET: CONFIGURATION-SET-NAME
Subject: Amazon SES Event Publishing Test
From: Amazon SES User <FROM-ADDRESS>
MIME-Version: 1.0
Content-Type: text/plain

This is a test message.
```

- Wählen Sie Send Test Email aus.
- Wiederholen Sie diese Schritte einige Male, damit Sie verschiedene E-Mail-Sendeereignisse generieren können. Ändern Sie bei mehreren E-Mails den Wert des Nachrichten-Tags `campaign` in `clothing`, um zu simulieren, dass die E-Mail für eine andere E-Mail-Kampagne gesendet wird. Wenn Sie dann im letzten Schritt dieses Tutorials die Datensätze für E-Mail-Sendeereignisse aus Ihrer Amazon Redshift t-Datenbank abfragen, können Sie verschiedene Abfragen auf Basis der E-Mail-Kampagne testen.

Nächster Schritt

[Schritt 7: E-Mail-Sendeereignissen \(p. 381\)](#)

Schritt 7: E-Mail-Sendeereignissen

Sie haben E-Mails mit Ihrem Konfigurationssatz und Nachrichten-Tags gesendet und auf diese Weise einige E-Mail-Sendeereignisse generiert. Nun können Sie diese Datensätze in Amazon Redshift abfragen.

Note

Es wird davon ausgegangen, dass SQL Workbench/J auf dem Computer ausgeführt wird und mit dem Amazon Redshift -Cluster verbunden ist, wie unter beschrieben. [Schritt 2: Connect Sie sich mit Ihrem Amazon Redshift Cluster \(p. 371\)](#).

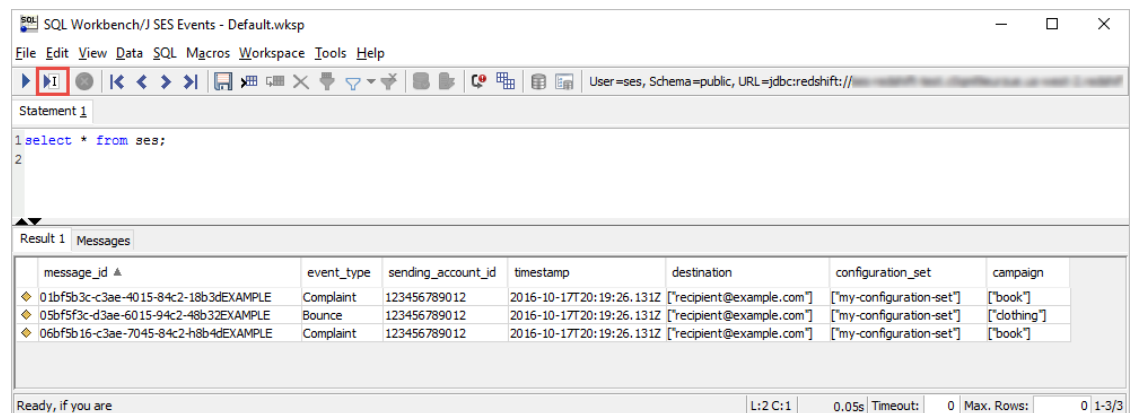
So fragen Sie Daten zu E-Mail-Sendeereignissen in Amazon Redshift ab

- Um alle E-Mail-Sendedatensätze anzuzeigen, kopieren Sie die folgende Abfrage und fügen Sie diese im Fenster Statement 1 ein.

```
select * from ses;
```

- Platzieren Sie den Cursor in der Anweisung (vor dem Semikolon) und klicken Sie auf Execute current statement.

Für alle E-Mails, die Sie unter [Schritt 6: Versenden von E-Mails \(p. 380\)](#) gesendet haben, werden die E-Mail-Sendedatensätze angezeigt. Die Datensätze in der folgenden Abbildung belegen, dass für die `book`-Kampagne zwei Beschwerden vorliegen und bei der `clothing`-Kampagne eine E-Mail unzustellbar war.



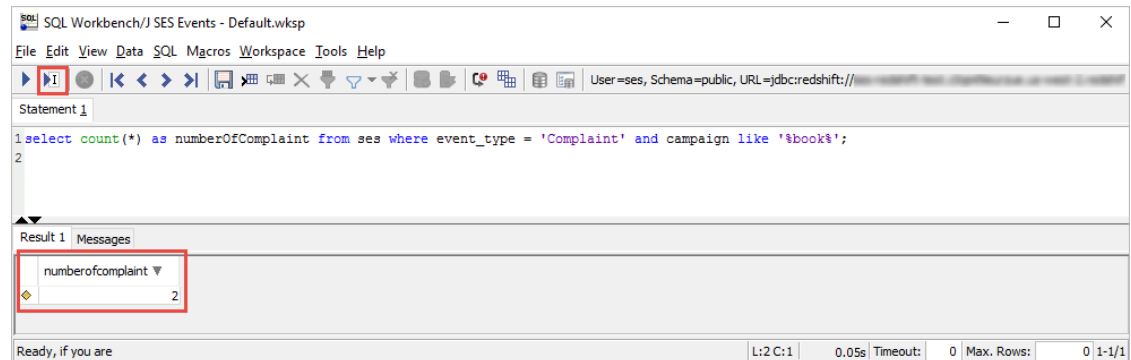
message_id	event_type	sending_account_id	timestamp	destination	configuration_set	campaign
01bf5b3c-c3ae-4015-84c2-18b3dEXAMPLE	Complaint	123456789012	2016-10-17T20:19:26.131Z	["recipient@example.com"]	["my-configuration-set"]	["book"]
05bf5f3c-d3ae-6015-94c2-48b32EXAMPLE	Bounce	123456789012	2016-10-17T20:19:26.131Z	["recipient@example.com"]	["my-configuration-set"]	["clothing"]
06bf5b16-c3ae-7045-84c2-h8b4dEXAMPLE	Complaint	123456789012	2016-10-17T20:19:26.131Z	["recipient@example.com"]	["my-configuration-set"]	["book"]

- Um die `complaint`-Datensätze für die `book`-Kampagne zu zählen, kopieren Sie die folgende Abfrage und fügen diese im Fenster Statement 1 ein.

```
select count(*) as numberOfComplaint from ses where event_type = 'Complaint' and  
campaign like '%book%';
```

4. Platzieren Sie den Cursor in der Anweisung (vor dem Semikolon) und klicken Sie auf Execute current statement.

Die Ergebnisse zeigen, dass für die "book"-Kampagne zwei Beschwerden vorhanden sind.



Darstellen von E-Mail-Sendeereignissen in Amazon CloudWatch

In diesem Tutorial veröffentlichen Sie E-Mail-Sendeereignisse von Amazon SES in Amazon CloudWatch und stellen anschließend die Ereignisse mithilfe der CloudWatch-Konsole grafisch dar.

In den folgenden Abschnitten finden Sie eine schrittweise Anleitung für dieses Verfahren.

- [Voraussetzungen \(p. 382\)](#)
- [Schritt 1: Einrichten eines Konfigurationssatzes \(p. 382\)](#)
- [Schritt 2: Versenden von E-Mails \(p. 383\)](#)
- [Schritt 3: Grafisches Ab \(p. 384\)](#)

Prerequisites

Für dieses Tutorial benötigen Sie Folgendes:

- Ein AWS-Konto Um auf alle von AWS bereitgestellten Webservices zuzugreifen, müssen Sie zunächst unter ein AWS-Konto erstellen <https://aws.amazon.com/>.
- bestätigte E-Mail-Adresse Verifizierte E-Mail-Adresse (Absender) oder Domäne, um E-Mails mit Amazon SES senden zu können, müssen Sie den Besitz ihrer E-Mail-Adresse (Absender) oder Domäne nachweisen. Falls Sie sich in einer Sandbox-Umgebung befinden, müssen auch die Empfängeradressen verifiziert werden. Sie können E-Mail-Adressen oder ganze Domänen verifizieren, jedoch ist in diesem Tutorial nur die Bestätigung einer E-Mail-Adresse erforderlich, damit Sie eine E-Mail über die Amazon SES Konsole versenden können (das ist die einfachste Möglichkeit, eine E-Mail zu senden). Weitere Informationen zum Verifizieren einer E-Mail-Adresse finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).

Nächster Schritt

[Schritt 1: Einrichten eines Konfigurationssatzes \(p. 382\)](#)

Schritt 1: Einrichten eines Konfigurationssatzes

Um Amazon SES so einzurichten, dass die E-Mail-Sendeereignisse in Amazon CloudWatch veröffentlicht werden, erstellen Sie zunächst einen Konfigurationssatz und fügen diesem dann ein CloudWatch-Ereignisziel hinzu. In diesem Abschnitt werden die dafür erforderlichen Schritte beschrieben.

Sofern Sie bereits über einen Konfigurationssatz verfügen, können Sie das CloudWatch Ziel zu diesem hinzufügen. Fahren Sie in diesem Falle mit [Hinzufügen eines CloudWatch Ereignisziels](#) (p. 383) fort.

Erstellen eines Konfigurationssatzes

Im folgenden Verfahren wird das Erstellen eines Konfigurationssatzes beschrieben.

So erstellen Sie einen Konfigurationssatz

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich Configuration Sets aus.
3. Wählen Sie Create Configuration Set aus.
4. Geben Sie einen Namen für den Konfigurationssatz ein und wählen Sie Create Configuration Set aus.

Hinzufügen eines CloudWatch Ereignisziels

Im folgenden Verfahren wird beschrieben, wie Sie ein CloudWatch Ereignisziel zum erstellten Konfigurationssatz hinzufügen.

So fügen Sie ein CloudWatch Ereignisziel zu einem Konfigurationssatz hinzu

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im Navigationsbereich Configuration Sets aus.
3. Wählen Sie den im vorigen Abschnitt erstellten Konfigurationssatz aus.
4. Für Ziel hinzufügen, wählen Sie Wählen Sie einen Zieltyp Klicken Sie auf und danach auf CloudWatch.
5. Geben Sie im Feld Name einen Namen für das Ereignisziel ein.
6. Für Ereignistypen Wählen Sie die Metriken aus, die Sie in Amazon CloudWatch melden möchten.
7. Wählen Sie Enabled (Aktiviert) aus.
8. Für Quelle des Wertes den Wert aus, den Sie verwenden möchten, um die Metriken in CloudWatch zu kategorisieren. Wenn Sie beispielsweise die Nachrichten-Tag Sie müssen ein Schlüssel-Wert-Paar angeben. Amazon SES sendet die ausgewählten Metriken an CloudWatch, wenn die E-Mail dieses Schlüssel-Wert-Paar als Nachrichten-Tag enthält. Wenn Sie die Metriken in CloudWatch anzeigen, werden sie anhand des Schlüssels des Nachrichten-Tags kategorisiert.

Note

Wenn Sie Verknüpfen mit Als Wertquelle können Sie Klickereignisse nur an CloudWatch senden. Sie können die Wertquelle Link Tag (Link-Tag) verwenden, um zu ermitteln, auf welche Links in Ihren E-Mails am häufigsten geklickt wird.

9. Wählen Sie Save (Speichern) aus.
10. Verwenden Sie die Zurück-Schaltfläche Ihres Browsers, um die Seite Edit Configuration Set zu verlassen.

Schritt 2: Versenden von E-Mails

Damit Amazon SES E-Mail-bezogene Ereignisse veröffentlicht, müssen Sie beim Senden der E-Mail einen Konfigurationssatz angeben. Sie können auch Nachrichten-Tags zur Kategorisierung der E-Mail einbinden. In diesem Abschnitt wird beschrieben, wie Sie mithilfe der Amazon SES -Konsole eine einfache E-Mail senden, in der ein Konfigurationssatz und Nachrichten-Tags angegeben sind. Sie senden die E-Mail an den Amazon SES Postfachsimulator, damit Sie Unzustellbarkeits-, Beschwerde- und andere E-Mail-Sendeergebnisse testen können.

So senden Sie eine E-Mail mit der Amazon SES Konsole

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. In der Navigation der Amazon SES Konsole unter Identitätsmanagement, wählen Sie E-Mail-Adressen.
3. Markieren Sie in der Liste der Identitäten eine E-Mail-Adresse, die erfolgreich für Sie [Bestätigt mit Amazon SES \(p. 52\)](#).
4. Wählen Sie Send a Test Email aus.
5. Wählen Sie im Dialogfeld Send Test Email im Feld Email Format die Option Raw aus.
6. Für die Bis-Adresse eine Adresse aus dem Feld [Amazon SES Postfach-Simulator \(p. 198\)](#), wie beispielsweise `complaint@simulator.amazonses.com` oder `bounce@simulator.amazonses.com`.
7. Kopieren Sie die gesamte folgende Nachricht und fügen Sie diese in das Textfeld Message (Nachricht) ein. Ersetzen Sie dabei `CONFIGURATION-SET-NAME` durch den Namen des Konfigurationssatzes, den Sie unter [Schritt 1: Einrichten eines Konfigurationssatzes \(p. 382\)](#) erstellt haben, und ersetzen Sie `FROM-ADDRESS` durch die verifizierte Adresse, von der Sie diese E-Mail senden.

```
X-SES-MESSAGE-TAGS: campaign=book
X-SES-CONFIGURATION-SET: CONFIGURATION-SET-NAME
Subject: Amazon SES Event Publishing Test
From: Amazon SES User <FROM-ADDRESS>
MIME-Version: 1.0
Content-Type: text/plain

This is a test message.
```

8. Wählen Sie Send Test Email aus.
9. Wiederholen Sie diese Schritte einige Male, damit Sie verschiedene E-Mail-Sendeereignisse generieren können. Ändern Sie bei mehreren E-Mails den Wert des Nachrichten-Tags `campaign` in `clothing`, um zu simulieren, dass die E-Mail für eine andere E-Mail-Kampagne gesendet wird.

Nächster Schritt

[Schritt 3: Grafisches Darstellen von E-Mail- \(p. 384\)](#)

Schritt 3: Grafisches Darstellen von E-Mail-

Sie haben E-Mails mit Ihrem Konfigurationssatz und Nachrichten-Tags gesendet und auf diese Weise einige E-Mail-Sendeereignisse von Amazon SES in CloudWatch veröffentlicht. Nun können Sie mithilfe der CloudWatch-Konsole Metriken für diese Ereignisse grafisch darstellen.

So stellen Sie Metriken für E-Mail-Sendeereignisse grafisch dar

1. Melden Sie sich beim an.AWS Management Console und öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im linken Navigationsbereich Metrics aus.
3. Wählen Sie auf der Registerkarte All metrics die Option SES aus.

Tip

Sie können auch `SES` in das Suchfeld eingeben.

4. Wählen Sie die Wertquelle aus, die Sie in [Hinzufügen eines CloudWatch Ereignisziels \(p. 383\)](#) angegeben haben. Wenn Sie beispielsweise das Nachrichten-Tag `"category: books"` als Wertquelle angegeben haben, wählen Sie `category` aus.
5. Wählen Sie die Metrik, die Sie anzeigen möchten. Im Detailbereich wird eine grafische Darstellung angezeigt.

Analysieren von E-Mail-Sendeereignissen mit Amazon Kinesis Data Analytics

Mit Amazon Kinesis Data Analytics können Sie Streaming-Daten mithilfe von SQL verarbeiten und analysieren. Sie können Amazon Kinesis Data Analytics verwenden, um Ihre Amazon SES E-Mail-Ereignisse zu analysieren.

In diesem Tutorial richten Sie zunächst einen Amazon SES Konfigurationssatz ein und veröffentlichen E-Mail-Sendeereignisse in einem Amazon Kinesis Data Firehose -Bereitstellungs-Stream. Dann senden Sie E-Mails mit Ihrem Konfigurationssatz über Amazon SES. Anschließend konfigurieren Sie Amazon Kinesis Data Analytics so, dass die E-Mail-Sendeereignisse aus dem Kinesis Data Firehose -Bereitstellungs-Stream erfasst werden, und extrahieren mithilfe von SQL wichtige Informationen aus den gesendeten E-Mails.

Note

Für dieses Tutorial ist eine Anwendung erforderlich, die einen konstanten E-Mail-Stream über Amazon SES senden kann. Diese Anforderung wird unter [Voraussetzungen \(p. 385\)](#) erklärt.

In den folgenden Abschnitten finden Sie eine schrittweise Anleitung für dieses Tutorial.

- [Voraussetzungen \(p. 385\)](#)
- [Schritt 1: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream. \(p. 386\)](#)
- [Schritt 2: Einrichten eines Konfigurationssatzes \(p. 387\)](#)
- [Schritt 3: Versenden von E-Mails \(p. 388\)](#)
- [Schritt 4: Erstellen einer Amazon Kinesis Data Analytics Anwendung \(p. 389\)](#)
- [Schritt 5: Ausführen einer SQL-Abfrage \(p. 393\)](#)
- (Optional) [Schritt 6: Speichern von SQL-Abfragefunk \(p. 395\)](#)

Prerequisites

Für dieses Tutorial benötigen Sie Folgendes:

- Ein AWS-Konto Um auf alle von AWS bereitgestellten Webservices zuzugreifen, müssen Sie zunächst unter ein AWS-Konto erstellen <https://aws.amazon.com/>.
- bestätigte E-Mail-Adresse Verifizierte E-Mail-Adresse (Absender) oder Domäne, um E-Mails mit Amazon SES senden zu können, müssen Sie den Besitz ihrer E-Mail-Adresse (Absender) oder Domäne nachweisen. Falls Sie sich in einer Sandbox-Umgebung befinden, müssen auch die Empfängeradressen verifiziert werden. Sie können E-Mail-Adressen oder ganze Domänen verifizieren, jedoch ist in diesem Tutorial nur die Bestätigung einer E-Mail-Adresse erforderlich, damit Sie eine E-Mail über die Amazon SES Konsole versenden können (das ist die einfachste Möglichkeit, eine E-Mail zu senden). Weitere Informationen zum Verifizieren einer E-Mail-Adresse finden Sie unter [Amazon Verifizieren von E-Mail-Adressen in Amazon SES \(p. 52\)](#).
- E-Mail-Anwendung— Um Amazon Kinesis Data Analytics gemäß dem Tutorial nutzen zu können, muss ein konstanter E-Mail-Stream über Amazon SES gesendet werden. Nur so lässt sich ein konstanter Stream aus E-Mail-Sendeereignissen erzeugen. Dadurch kann Amazon Kinesis Data Analytics das Schema automatisch erkennen und die Ereignisdatensätze mit SQL verarbeiten. Es reicht in diesem Tutorial aus, fünf Minuten lang alle zehn Sekunden eine E-Mail zu senden.

Important

Sofern Sie keine E-Mail-Kampagne mit echten Empfängern haben, wird empfohlen, die E-Mails an einen [Amazon SES Postfach-Simulator \(p. 198\)](#) Adresse. An den Postfachsimulator gesendete E-Mails werden nicht in Ihre Unzustellbarkeits- und Beschwerdequoten für Amazon SES oder in Ihre tägliche Sendequote eingerechnet.

Nächster Schritt

Schritt 1: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream. (p. 386)

Schritt 1: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream.

Um Amazon SES E-Mails zu analysieren, die Ereignisse mit Amazon Kinesis Data Analytics senden, müssen Sie Amazon SES so konfigurieren, dass die Ereignisse in einem Amazon Kinesis Data Firehose Delivery Stream veröffentlicht werden, und dann Amazon Kinesis Data Analytics so konfigurieren, dass die Ereignisdaten aus Kinesis Data Firehose abgerufen werden.

Beim Einrichten des -Bereitstellungs-Stream von Kinesis Data Firehose wählen Sie den Zielort für die Daten aus. Ihre Zieloptionen sind Amazon Simple Storage Service (Amazon S3), Amazon Elasticsearch Service und Amazon Redshift. Wenn Sie einfach nur E-Mail-Sendeereignisse mit Amazon Kinesis Data Analytics analysieren möchten, ist das Ziel belanglos. In diesem Tutorial wird Kinesis Data Firehose so konfiguriert, dass die Daten in Amazon S3 veröffentlicht werden. Sie können auch die anderen Ziele verwenden, sofern diese in derselben Region sind wie der -Sende-Stream und der Kinesis Data Firehose -Bereitstellungs-Stream.

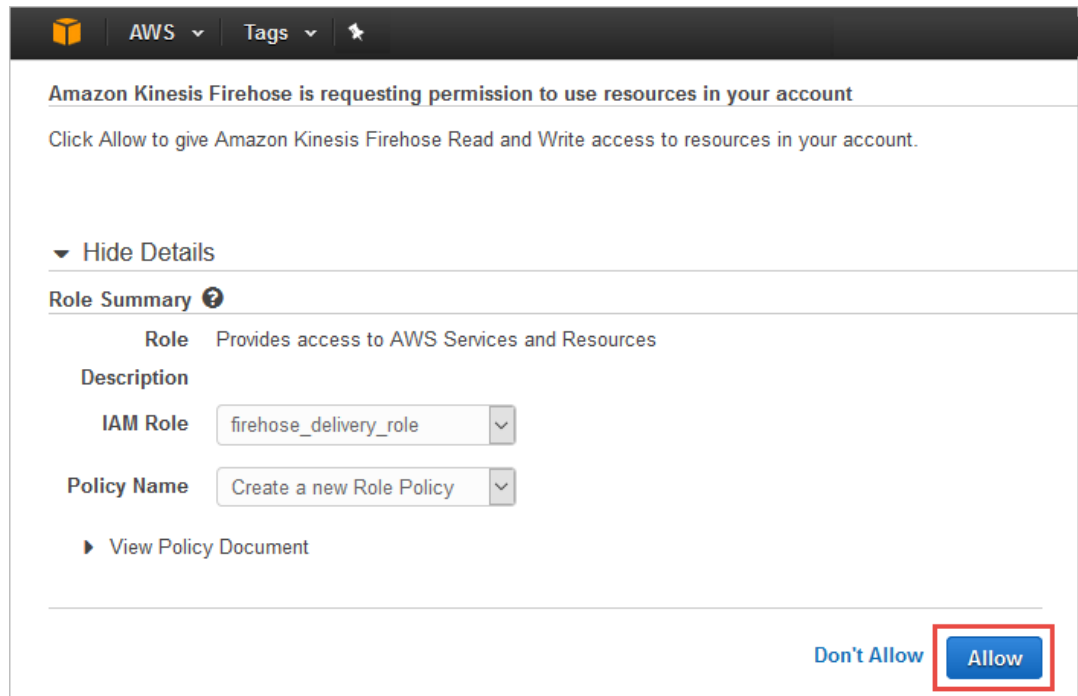
In diesem Abschnitt wird gezeigt, wie Sie einen Kinesis Data Firehose Delivery Stream mit der Kinesis Data Firehose Konsole erstellen. In diesem Tutorial werden nur die grundlegenden Optionen ausgewählt. Weitere Informationen zu allen verfügbaren Optionen finden Sie unter [Erstellen eines Amazon Kinesis Firehose Bereitstellungs-Streams](#) im Entwicklerhandbuch für Amazon Kinesis Data Firehose.

So erstellen Sie einen Lieferdatenstrom von Kinesis Data Firehose zu Amazon S3

1. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Kinesis Data Firehose Konsole unter<https://console.aws.amazon.com/firehose/>.
2. Wählen Sie Create Delivery Stream aus.
3. Wählen Sie auf der Seite Destination die folgenden Optionen aus.
 - Zielbereich— Auswählen vonAmazon S3.
 - Delivery stream name – Geben Sie einen Namen für den Bereitstellungs-Stream an.
 - S3 bucket— Wählen Sie einen vorhandenen Bucket aus oder klicken Sie aufNeuer S3-Bucket. Wenn Sie einen neuen Bucket erstellen, geben Sie einen Bucket-Namen ein und wählen Sie die Region aus, die derzeit von der Konsole verwendet wird.
 - S3 prefix – Dieses Feld bleibt leer.
4. Wählen Sie Next.
5. Übernehmen Sie auf der Seite Configuration die Standardeinstellungen der Felder. Sie müssen hier nur eine IAM-Rolle auswählen, um Kinesis Data Firehose den Zugriff auf Ihre Ressourcen zu gewähren, wie im folgenden Verfahren beschrieben:
 - a. Wählen Sie im Feld IAM Role die Option Select an IAM role aus.
 - b. Wählen Sie im Dropdown-Menü unter Create/Update existing IAM role den Eintrag Firehose delivery IAM role aus.

Sie werden zur IAM-Konsole umgeleitet.

- c. Übernehmen Sie in der IAM-Konsole die Standardeinstellungen der Felder und klicken Sie auf der IAM-Konsole aufSobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf.



In der Kinesis Data Firehose Konsole kehren Sie zu den Einrichtungsschritten des - Bereitstellungs-Streams zurück.

6. Wählen Sie Next.
7. Prüfen Sie auf der Seite Review Ihre Einstellungen und wählen Sie Create Delivery Stream aus.

Nächster Schritt

[Schritt 2: Einrichten eines Konfigurationssatzes \(p. 387\)](#)

Schritt 2: Einrichten eines Konfigurationssatzes

Um so einzurichten, dass die E-Mail-Sendeereignisse in Amazon Kinesis Data Firehose veröffentlicht werden, erstellen Sie einen Konfigurationssatz und fügen diesem dann ein -Ereignisziel hinzu. In diesem Abschnitt werden die dafür erforderlichen Schritte beschrieben.

Sofern Sie bereits über einen Konfigurationssatz verfügen, können Sie das Kinesis Data Firehose-Ziel zu diesem hinzufügen. Fahren Sie in diesem Falle mit [Hinzufügen eines Kinesis Data Firehose Ereignisziels \(p. 388\)](#) fort.

Erstellen eines Konfigurationssatzes

Im folgenden Verfahren wird das Erstellen eines Konfigurationssatzes beschrieben.

So erstellen Sie einen Konfigurationssatz

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon SES Konsole unter <https://console.aws.amazon.com/ses/>.
2. Wählen Sie im linken Navigationsbereich Configuration Sets aus.
3. Wählen Sie im Inhaltsbereich Create Configuration Set aus.
4. Geben Sie einen Namen für den Konfigurationssatz ein und wählen Sie Create Configuration Set aus.

5. Klicken Sie auf Close.

Hinzufügen eines Kinesis Data Firehose Ereignisziels

Im folgenden Verfahren wird beschrieben, wie Sie ein Kinesis Data Firehose-Ereignisziel zum erstellten Konfigurationssatz hinzufügen.

So fügen Sie ein Kinesis Data Firehose Ereignisziel zum Konfigurationssatz hinzu

1. Wählen Sie den Konfigurationssatz aus der Liste der Konfigurationssätze aus.
2. Für Ziel hinzufügen, wählen Sie Wählen Sie einen Zieltyp Klicken Sie auf und danach auf Kinesis Data Firehose.
3. Geben Sie im Feld Name einen Namen für das Ereignisziel ein.
4. Wählen Sie alle Einträge unter Event types aus.
5. Wählen Sie Enabled.
6. Wählen Sie im Feld Stream den Bereitstellungs-Stream aus, den Sie unter [Schritt 1: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream. \(p. 386\)](#) erstellt haben.
7. Wählen Sie im Feld IAM role die Option Let SES make a new role aus und geben Sie dann einen Namen für die Rolle ein.
8. Wählen Sie Save (Speichern) aus.
9. Verwenden Sie die Zurück-Schaltfläche Ihres Browsers, um die Seite Edit Configuration Set zu verlassen.

Nächster Schritt

[Schritt 3: Versenden von E-Mails \(p. 388\)](#)

Schritt 3: Versenden von E-Mails

Da in diesem Tutorial die Amazon Kinesis Data Analytics Konsole zur Verarbeitung und Analyse der Streaming-Daten verwendet wird, muss ein konstanter E-Mail-Stream über Amazon SES eingerichtet werden. In diesem Tutorial wird davon ausgegangen, dass Sie über eine Anwendung verfügen, die diese E-Mails senden kann. Es reicht in diesem Tutorial aus, fünf Minuten lang alle zehn Sekunden eine E-Mail zu senden. Am besten verwenden Sie eine Empfängeradresse des [Amazon SES Postfach-Simulator \(p. 198\)](#), wie beispielsweise `success@simulator.amazonses.com`.

Um die Ereignisveröffentlichung für eine E-Mail zu aktivieren, übergeben Sie beim Senden der E-Mail den Namen des Konfigurationssatzes an Amazon SES. Optional können Sie Nachrichten-Tags zur Kategorisierung der E-Mail einbinden. Diese Informationen stellen Sie Amazon SES entweder als Parameter an die E-Mail sendende API, als Amazon SES-spezifischer E-Mail-Header oder als benutzerdefinierter Header in Ihrer MIME-Nachricht bereit. Weitere Informationen finden Sie unter [Senden einer E-Mail mithilfe der Amazon SES-Ereignisveröffentlichung \(p. 323\)](#).

Beispielsweise können Sie der E-Mail die folgenden Amazon SES-spezifischen E-Mail-Header hinzufügen, um eine „book“-Kampagne zu simulieren. Ersetzen Sie `CONFIGURATION-SET-NAME` durch den Namen des Konfigurationssatzes, den Sie unter [Schritt 2: Einrichten eines Konfigurationssatzes \(p. 387\)](#) erstellt haben.

```
X-SES-CONFIGURATION-SET: CONFIGURATION-SET-NAME
X-SES-MESSAGE-TAGS: campaign=book
```

Nächster Schritt

[Schritt 4: Erstellen einer Amazon Kinesis Data Analytics Anwendung \(p. 389\)](#)

Schritt 4: Erstellen einer Amazon Kinesis Data Analytics Anwendung

Nun, da Sie die -Ereignisveröffentlichung mit Amazon SES eingerichtet haben, können Sie Amazon Kinesis Data Analytics so konfigurieren, dass Daten der E-Mail-Sendeereignisse aus dem Amazon Kinesis Data Firehose -Bereitstellungs-Stream abgerufen werden. Dazu erstellen Sie eine Amazon Kinesis Data Analytics Anwendung.

Im folgenden Verfahren wird beschrieben, wie Sie mithilfe der Amazon Kinesis Data Analytics Konsole eine Anwendung erstellen, die Daten der E-Mail-Sendeereignisse von Amazon SES aus dem -Kinesis Data Firehose -Bereitstellungs-Stream erfasst. Zudem erfahren Sie, wie Sie eine einfache SQL-Abfrage für diese Daten ausführen, um Ereignisse des Typs „Send“ zu erhalten.

Note

Die E-Mail-Sendeereignisse der verschiedenen Ereignistypen ("Send", "Bounce", "Complaint" und "Delivery") haben auch [unterschiedliche JSON-Schemata \(p. 328\)](#). In einer Produktionsumgebung sind möglicherweise mehrere Felder dieses Schema vorhanden, aber in diesem Tutorial werden nur ein paar Felder verwendet, die für alle Ereignistypen vorhanden sind.

So erstellen Sie eine Amazon Kinesis Data Analytics Anwendung

1. Beginnen Sie damit, einen konstanten Stream an E-Mails mit konfigurierter Amazon SES zu senden. Senden Sie während dieses ganzen Verfahrens weiterhin E-Mails. Das ist erforderlich, damit Amazon Kinesis Data Analytics das Schema der Ereignisdatensätze automatisch erkennen kann. Es reicht in diesem Tutorial aus, fünf Minuten lang alle zehn Sekunden eine E-Mail zu senden. Weitere Informationen finden Sie unter [Schritt 3: Versenden von E-Mails \(p. 388\)](#).

Wenn das E-Mail-Programm einige E-Mails gesendet hat, fahren Sie mit dem nächsten Schritt fort.

2. Melden Sie sich beim an.AWS Management Consoleund öffnen Sie die Kinesis Data Analytics Konsole unter<https://console.aws.amazon.com/kinesisanalytics>.
3. Wählen Sie Create new application.
4. Geben Sie einen Anwendungsnamen und eine Beschreibung ein und klicken Sie dann auf Save and continue.
5. Klicken Sie auf Connect to a source.
6. Wählen Sie den Kinesis Data Firehose Stream aus, den Sie in[Schritt 2: Einrichten eines Konfigurationssatzes \(p. 387\)](#).

Amazon Kinesis Data Analytics versucht, das Datensatzschema für das E-Mail-Sendeereignis auf Basis der eingehenden Datensätze zu ermitteln. Wenn Amazon Kinesis Data AnalyticsFehler beim Ermitteln des EingabeschemasDas bedeutet, dass Amazon Kinesis Data Analytics bisher noch keine E-Mail-Sendedatensätze empfangen hat. Klicken Sie auf Rediscover schema. Möglicherweise müssen Sie mehrfach auf diese Schaltfläche klicken. Wenn die Schemaerkennung auch nach mehreren Versuchen nicht erfolgreich ist, prüfen Sie, ob Ihre Anwendung konstant E-Mails sendet und ob in den E-Mails ein Konfigurationssatz spezifiziert wird.

Wenn Amazon Kinesis Data Analytics ein Schema erkennt, wird eine Erfolgsmeldung angezeigt. Zudem werden die erkannten Datensätze aufgelistet.

Important

Klicken Sie nicht auf Save and continue. Das würde Fehler verursachen, da das erkannte Schema nicht den SQL-Benennungseinschränkungen entspricht. Sie müssen das Schema wie im nächsten Schritt beschrieben bearbeiten.

7. Wählen Sie Edit schema.

✓ **Schema discovery successful**
Detected JSON format and applied schema

- To define a custom schema, choose "Edit schema" in the stream sample below.
- To capture a new stream sample from the selected source for discovery, [rediscover the schema](#)

(Optional) Send AWS a sample of your data to help improve schema discovery in Amazon Kinesis Analytics

[Help improve schema discovery](#)

Formatted stream sampleRaw stream sample

Filter by column name or column type

Edit schema

messageId0 VARCHAR(64)	eventType VARCHAR(8)	source VARCHAR(32)	sourceArn VARCHAR(128)
EXAMPLE8d633ffe4-9d79e202-8e68-4d84-8c12-bd80644b270e-000000	Send	sender@example.com	arn:aws:ses:us-east-
EXAMPLE8d633ffe4-9d79e202-8e68-4d84-8c12-bd80644b270e-000000	Send	sender@example.com	arn:aws:ses:us-east-
EXAMPLE8d633ffe4-9d79e202-8e68-4d84-8c12-bd80644b270e-000000	Send	sender@example.com	arn:aws:ses:us-east-
EXAMPLE8d633ffe4-9d79e202-8e68-4d84-8c12-bd80644b270e-000000	Send	sender@example.com	arn:aws:ses:us-east-
EXAMPLE8d633ffe4-9d79e202-8e68-4d84-8c12-bd80644b270e-000000	Send	sender@example.com	arn:aws:ses:us-east-
EXAMPLE8d633ffe4-9d79e202-8e68-4d84-8c12-bd80644b270e-000000	Send	sender@example.com	arn:aws:ses:us-east-

8. In diesem Tutorial werden die meisten Zeilen entfernt. Klicken Sie auf das X neben allen Zeilen – außer bei Zeilen mit folgenden Spaltennamen:

- eventType
- timestamp
- messageId
- to
- ses:configuration-set

Important

Klicken Sie nicht auf Save schema and update stream samples. Das würde Fehler verursachen, da das erkannte Schema nicht den SQL-Benennungseinschränkungen entspricht. Sie müssen das Schema wie im nächsten Schritt beschrieben bearbeiten.

Kinesis Analytics dashboard > Example > Source > Edit schema

Format: JSON Record encoding: UTF-8 Row path: \$

Filter by column name

	Column order	Column name	Column type	Length	Row path
+ Add column					
☒	1	eventType	VARCHAR	8	\$.eventType
☒	2	timestamp	TIMESTAMP		\$.mail.timestamp
☒	3	source	VARCHAR	32	\$.mail.source
☒	4	sourceArn	VARCHAR	128	\$.mail.sourceArn
☒	5	sendingAccountId	BIGINT		\$.mail.sendingAcco
☒	6	messageId	VARCHAR	64	\$.mail.messageId
☒	7	destination	VARCHAR	64	\$.mail.destination[

9. Überprüfen Sie die verbleibenden Einträge unter Column name und vergleichen Sie diese wie folgt mit den SQL-Benennungseinschränkungen:
 - Format— Wie in [IDsimSQL-Referenz](#) für Amazon Kinesis Data Analytics Ohne Anführungszeichen angegebene IDs müssen mit einem Buchstaben oder Unterstrich beginnen, gefolgt von Buchstaben, Ziffern oder Unterstrichen. Die automatischen Tag-Namen von Amazon SES enthalten Kommas und Bindestriche und entsprechen damit nicht diesen Anforderungen. Sie werden diese im nächsten Schritt bearbeiten.
 - Reservierte Wörter Reservierte SQL-Wörter dürfen keinen Konflikt mit den reservierten SQL-Wörtern verursachen, die unter aufgeführt sind [Reservierte Wörter und Schlüsselwörter](#) im SQL-Referenz für Amazon Kinesis Data Analytics. Beispiele für reservierte Schlüsselwörter, die in Konflikt mit den Amazon SES Ereignisdatensätzen `timestamp`, `value`, `date`, `from`, und `to`.
10. Ändern Sie die verbleibenden Spaltennamen wie folgt, damit sie den SQL-Anforderungen entsprechen:
 - Benennen Sie `ses:configuration-set` um zu `ses_configuration_set`.
 - Benennen Sie `timestamp` um zu `ses_timestamp`.
 - Benennen Sie `to` um zu `ses_to`.

Kinesis Analytics dashboard > Example > Source > Edit schema

Format: JSON Record encoding: UTF-8 Row path: \$

Filter by column name

	Column order	Column name	Column type	Length	Row path
+	1	eventType	VARCHAR	8	\$.eventType
+	2	ses_timestamp	TIMESTAMP		\$.mail.timestamp
+	3	messageId	VARCHAR	64	\$.mail.messageId
+	4	ses_to	VARCHAR	64	\$.mail.commonHeader
+	5	ses_configuration_set	VARCHAR	16	\$.mail.tags.ses.config

Cancel Save schema and update stream samples

- Klicken Sie auf Save schema and update stream samples. Falls Validierungsfehler auftreten, stellen Sie sicher, dass Sie Schritt 10 korrekt ausgeführt haben. Wenn die Fehlermeldung No rows in source stream angezeigt wird, stellen Sie sicher, dass Sie immer noch den E-Mail-Stream senden, den Sie zu Beginn dieses Verfahrens gestartet haben. Klicken Sie dann auf Retrieve rows. Möglicherweise müssen Sie Abrufen von Zeilen mehrere Male, bevor Amazon Kinesis Data Analytics Datensätze erfasst.
- Nach einem erfolgreichen Zeilenabruf klicken Sie auf Exit (done).

Filter by column name

	Column order	Column name	Column type	Length	Row path
+	1	eventType	VARCHAR	8	\$.eventType
+	2	ses_timestamp	TIMESTAMP		\$.mail.timestamp
+	3	messageId	VARCHAR	64	\$.mail.messageId
+	4	ses_to	VARCHAR	64	\$.mail.commonHeader
+	5	ses_configuration_set	VARCHAR	16	\$.mail.tags.ses.config

Exit (done) Save schema and update stream samples

Nächster Schritt

Schritt 5: Ausführen einer SQL-Abfrage (p. 393)

Schritt 5: Ausführen einer SQL-Abfrage

Sie haben eine Amazon Kinesis Data Analytics Anwendung erstellt und so konfiguriert, dass sie den Amazon Kinesis Data Firehose -Bereitstellungs-Stream als Quelle verwendet. Nun können Sie die Ereignisdaten der E-Mail-Sendeereignisse abfragen, die der Kinesis Data Firehose -Bereitstellungs-Stream erhält.

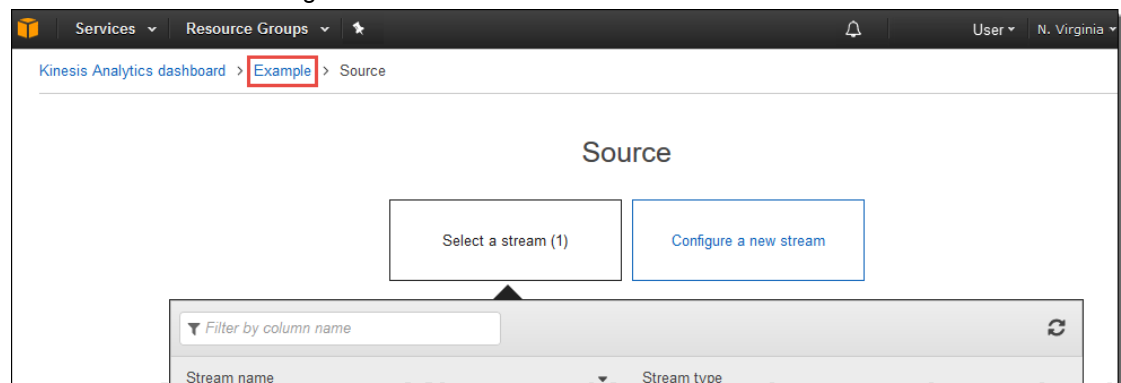
In diesem Thema wird beschrieben, wie Sie eine SQL-Abfrage für die Daten der E-Mail-Sendeereignisse ausführen.

Important

Für dieses Verfahren ist es erforderlich, weiterhin einen konstanten Stream an E-Mails mit konfigurierter -Ereignisveröffentlichung Amazon SES, wie unter beschrieben.[Schritt 3: Versenden von E-Mails](#) (p. 388).

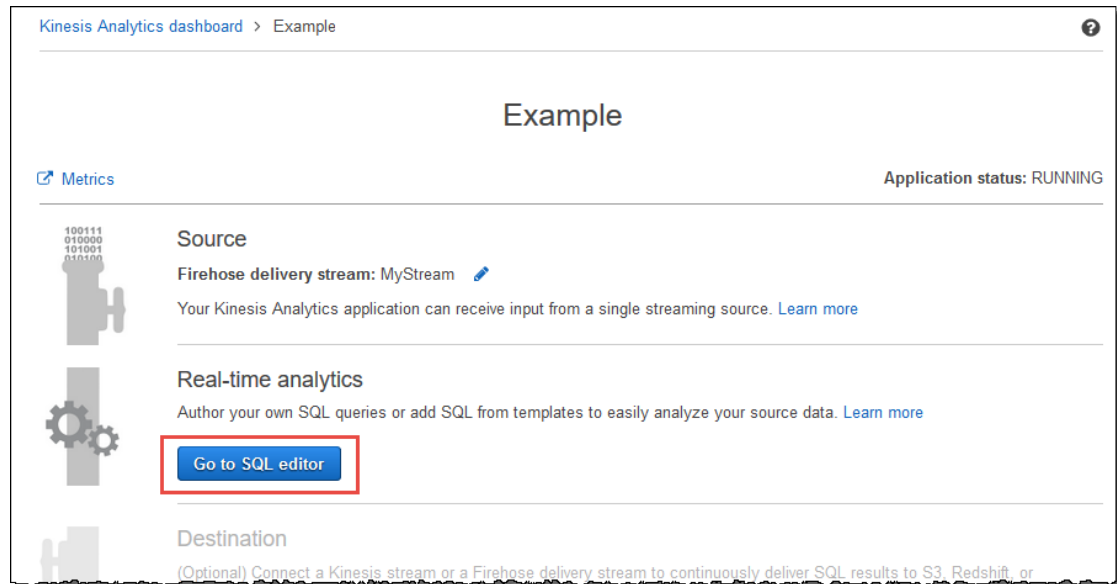
So führen Sie eine SQL-Abfrage in Amazon Kinesis Data Analytics aus

1. Es wird davon ausgegangen, dass Sie nach Abschluss des -Befehls mit diesem Punkt weitermachen.[letzter Schritt](#) (p. 389) Rufen Sie die Amazon Kinesis Data Analytics Konsole auf und wählen Sie Ihre Anwendung aus.



2. Klicken Sie auf Go to SQL editor.

Amazon Kinesis Data Analytics versucht, Ereignisdaten aus dem Kinesis Data Firehose Stream zu lesen. Wenn die Fehlermeldung No rows in source stream angezeigt wird, stellen Sie sicher, dass Sie immer noch den E-Mail-Stream senden, den Sie zu Beginn dieses Verfahrens gestartet haben. Klicken Sie dann auf Retrieve rows.



3. Geben Sie folgende Sequenz in den Code-Editor ein.

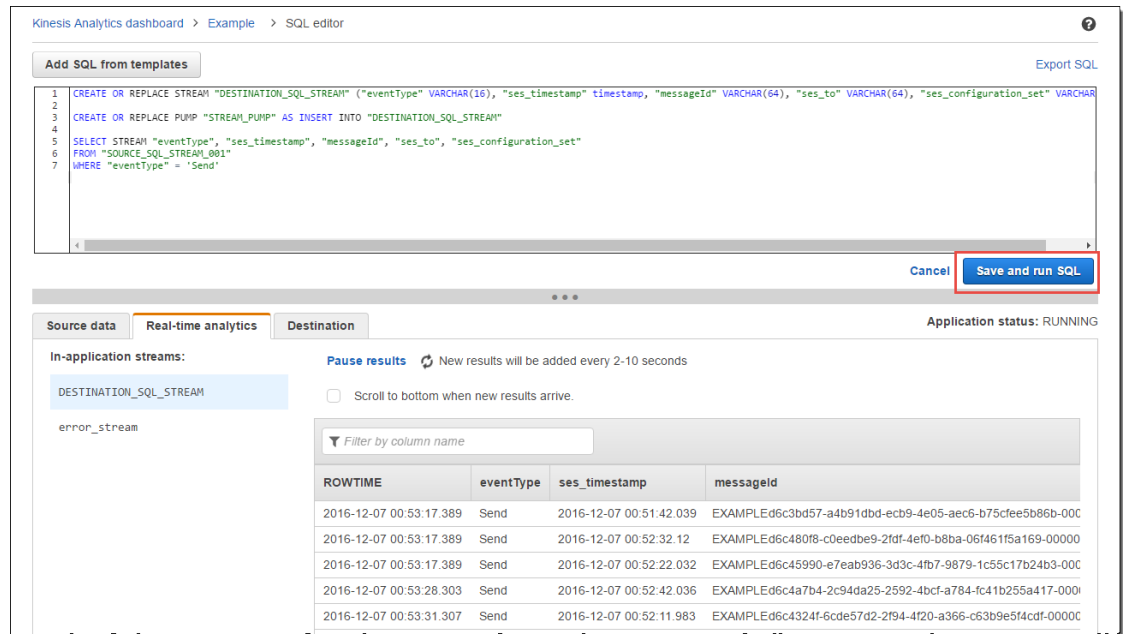
```
CREATE OR REPLACE STREAM "DESTINATION_SQL_STREAM" ("eventType" VARCHAR(16),
"ses_timestamp" timestamp, "messageId" VARCHAR(64), "ses_to" VARCHAR(64),
"ses_configuration_set" VARCHAR(32));

CREATE OR REPLACE PUMP "STREAM_PUMP" AS INSERT INTO "DESTINATION_SQL_STREAM"

SELECT STREAM "eventType", "ses_timestamp", "messageId", "ses_to",
"ses_configuration_set"
FROM "SOURCE_SQL_STREAM_001"
WHERE "eventType" = 'Send'
```

4. Klicken Sie auf Save and run SQL.

Nachdem Amazon Kinesis Data Analytics eingehende Datensätze empfängt und verarbeitet, wird eine Liste von Ereignisdatsätzen des Typs „Send“ angezeigt.



Nächster Schritt

(Optional) Schritt 6: Speichern von SQL-Abfragefunk (p. 395)

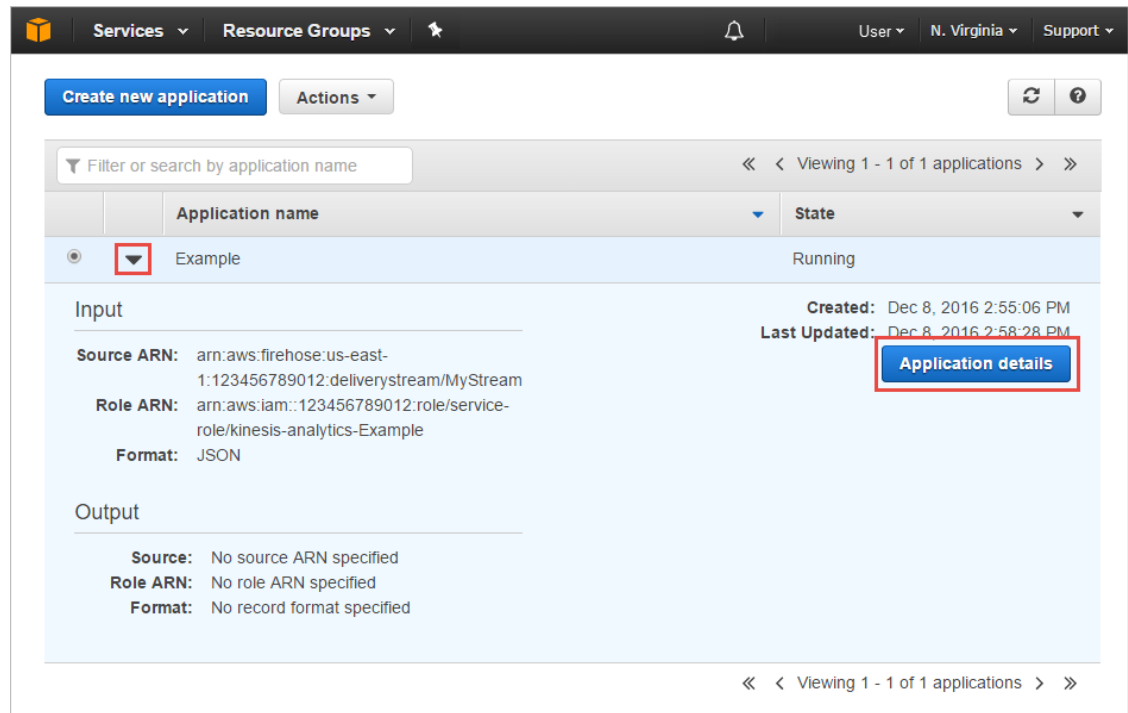
(Optional) Schritt 6: Speichern von SQL-Abfragefunk

Sie können Ihre Amazon Kinesis Data Analytics Anwendung so konfigurieren, dass die Ausgabe Ihrer SQL-Abfragen in einen Amazon Kinesis Data Firehose -Bereitstellungs-Stream geschrieben wird. Dazu müssen Sie einen weiteren -Bereitstellungs-Stream für Kinesis Data Firehose erstellen, da nicht ein und derselbe Bereitstellungs-Stream als Quelle und als Ziel der Amazon Kinesis Data Analytics Anwendung verwendet werden kann. Wie bei jedem Kinesis Data Firehose -Bereitstellungs-Stream können Sie Amazon Simple Storage Service (Amazon S3), Amazon Elasticsearch Service oder Amazon Redshift als Ziel auswählen.

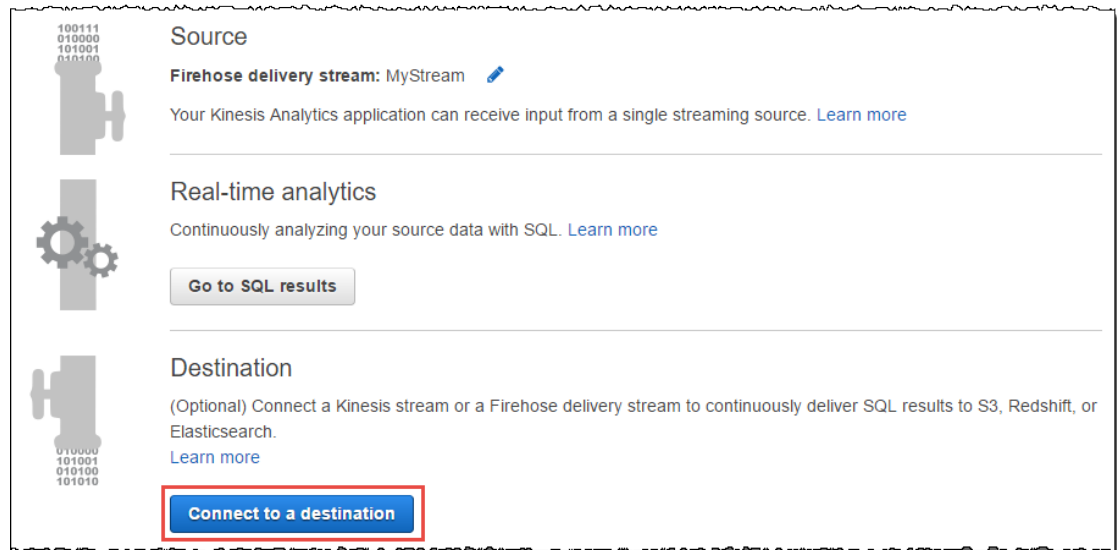
Im folgenden Verfahren wird beschrieben, wie Sie Amazon Kinesis Data Analytics so konfigurieren, dass die SQL-Abfrageergebnisse im JSON-Format in einem Kinesis Data Firehose -Bereitstellungs-Stream gespeichert werden, der die Daten in Amazon S3 schreibt. Dann führen Sie eine SQL-Abfrage aus und rufen die gespeicherten Daten auf.

So speichern Sie SQL-Abfrageergebnisse in Amazon S3

1. Richten Sie einen neuen Kinesis Data Firehose Stream mit Amazon S3 als Ziel ein. Dies ist dasselbe Verfahren wie unter [Schritt 1: Erstellt einen Kinesis Data Firehose-Bereitstellungs-Stream.](#) (p. 386) beschrieben.
2. Rufen Sie auf [Amazon Kinesis Data Analytics Konsole](#) Wählen Sie den Pfeil neben Ihrer Anwendung aus und klicken Sie auf [Anwendungsdetails](#).



3. Klicken Sie auf Connect to a destination.



4. Wählen Sie den unter Schritt 1 erstellten Kinesis Data Firehose -Stream aus und übernehmen Sie für die anderen Optionen die Standardeinstellungen. Klicken Sie dann auf Speichern und fortfahren.

Nach einigen Sekunden werden Sie zur Hauptseite der Anwendung zurückgeleitet.

Destination

Select a stream (1) [Configure a new stream](#)

Stream name	Stream type
StreamForSQL	Firehose delivery stream

In your SQL, refer to this stream as `DESTINATION_SQL_STREAM`

Output format: JSON

Permission to access the stream: ☒ Create/update Example IAM role ☐ Choose an IAM role

[Cancel](#) [Save and continue](#)

5. Klicken Sie auf Go to SQL results.

Source

Firehose delivery stream: MyStream

Your Kinesis Analytics application can receive input from a single streaming source. [Learn more](#)

Real-time analytics

Continuously analyzing your source data with SQL. [Learn more](#)

[Go to SQL results](#)

Destination

Firehose delivery stream: StreamForSQL

Connect a Kinesis Stream, or a Firehose delivery stream to continuously deliver SQL results to S3, Redshift or Elasticsearch. [Learn more](#)

6. Klicken Sie auf Save and run SQL, um die unter [Schritt 5: Ausführen einer SQL-Abfrage \(p. 393\)](#) erfolgte Abfrage erneut auszuführen.

Amazon Kinesis Data Analytics versucht, die erhaltenen Ereignisdaten aus dem Kinesis Data Firehose hose-Bereitstellungs-Stream zu lesen. Wenn Sie auf dieEs sind noch keine Zeilen eingetroffenVergewissern Sie sich, dass Sie immer noch E-Mails senden, sodass Amazon Kinesis Data Analytics E-Mail-Versandereignisse zur Verarbeitung vorliegen.

Wenn Amazon Kinesis Data Analytics Datensätze verarbeitet, werden die Ergebnisse im Echtzeit-Analysenregisterkarte. Amazon Kinesis Data Analytics speichert die Ergebnisse automatisch in dem Amazon S3 Bucket, den Sie beim Einrichten des Kinesis Data Firehose unter Schritt 1 angegeben haben.

The screenshot shows the Amazon Kinesis Data Analytics console. At the top, there's a navigation bar with 'Kinesis Analytics dashboard', 'Example', and 'SQL editor'. Below this is a 'SQL editor' tab with a text area containing SQL code. The code is as follows:

```
1 CREATE OR REPLACE STREAM "DESTINATION_SQL_STREAM" ("eventType" VARCHAR(16), "ses_timestamp" timestamp, "messageId" VARCHAR(64), "ses_to" VARCHAR(64), "ses_configuration_set" VARCHAR(64))
2
3 CREATE OR REPLACE PUMP "STREAM_PUMP" AS INSERT INTO "DESTINATION_SQL_STREAM"
4
5 SELECT STREAM "eventType", "ses_timestamp", "messageId", "ses_to", "ses_configuration_set"
6 FROM "SOURCE_SQL_STREAM_001"
7 WHERE "eventType" = 'Send'
```

Below the SQL editor, there are 'Cancel' and 'Save and run SQL' buttons. The 'Save and run SQL' button is highlighted with a red box. Below this, there's a 'Real-time analytics' tab. It shows 'In-application streams' with 'DESTINATION_SQL_STREAM' selected. There's a 'Pause results' button and a checkbox 'Scroll to bottom when new results arrive'. Below this is a table with the following data:

ROWTIME	eventType	ses_timestamp	messageId
2016-12-07 00:53:17.389	Send	2016-12-07 00:51:42.039	EXAMPLEd6c3bd57-a4b91dbd-ecb9-4e05-aec6-b75cfee5b86b-000
2016-12-07 00:53:17.389	Send	2016-12-07 00:52:32.12	EXAMPLEd6c480f8-c0eedbe9-2fdf-4ef0-b8ba-06f461f5a169-00000
2016-12-07 00:53:17.389	Send	2016-12-07 00:52:22.032	EXAMPLEd6c45990-e7eab936-3d3c-4fb7-9879-1c55c17b24b3-000
2016-12-07 00:53:28.303	Send	2016-12-07 00:52:42.036	EXAMPLEd6c4a7b4-2c94da25-2592-4bcf-a784-fc41b255a417-000i
2016-12-07 00:53:31.307	Send	2016-12-07 00:52:11.983	EXAMPLEd6c4324f-6cde57d2-2f94-4f20-a366-c53b9e5f4cdf-00000

- Öffnen Sie zum Abrufen der Ergebnisse das Dialogfeld [Amazon S3-Konsole](#).
- Wählen Sie den Amazon S3 Bucket aus, der dem Kinesis Data Firehose se-Bereitstellungsstream zugeordnet ist, den die Amazon Kinesis Data Analytics Anwendung als Ziel verwendet.
- Navigieren Sie zu den Daten, die standardmäßig basierend auf dem Datum, an dem die Ergebnisse im Bucket gespeichert wurden, in einer Ordnerhierarchie sortiert sind.

Falls der Bucket leer ist, warten Sie einige Minuten und versuchen Sie es erneut. Es kann einige Minuten dauern, bis die Amazon Kinesis Data Analytics in Ihren Amazon S3 Bucket ankommen.

- Wählen Sie eine Datei aus und klicken Sie im Menü Actions auf Download.

The screenshot shows the Amazon S3 console. At the top, there's a navigation bar with 'Services', 'Resource Groups', and a search bar. Below this is a 'Bucket' view for 'example'. It shows a list of files with columns 'Name', 'Storage Class', 'Size', and 'Last Modified'. The files are:

Name	Storage Class	Size	Last Modified
StreamForSQL-1-2016-12-07-00:53:17.389	Standard	6.2 KB	Thu Dec 08 15:51:50 GMT-800 2016
StreamForSQL-1-2016-12-07-00:53:28.303	Standard	6.9 KB	Thu Dec 08 15:56:55 GMT-800 2016

Below the list, there's an 'Actions' menu. The 'Download' option is highlighted with a red box. Other options in the menu include 'Open', 'Create Folder...', 'Upload', 'Make Public', 'Rename', 'Delete', 'Initiate Restore', 'Cut', 'Copy', 'Paste', and 'Properties'.

11. Folgen Sie den Anweisungen auf dem Bildschirm, um die Datei auf den Computer herunterzuladen.
12. Öffnen Sie die Datei auf Ihrem Computer mit einem Texteditor. Es handelt sich um Datensätze im JSON-Format, die in geschweiften Klammern stehen. Nachfolgend finden Sie eine Beispieldatei mit zwei Datensätzen.

```
{ "eventType": "Send", "ses_timestamp": "2016-12-08
  18:51:12.092", "messageId": "EXAMPLE8dfc6695c-5f048b74-
ca83-4052-8348-4e7da9669fc3-000000", "ses_to": "[\"success@simulator.amazonses.com
\" ]", "ses_configuration_set": "[\"MyConfigSet\" ]"}
{ "eventType": "Send", "ses_timestamp": "2016-12-08
  18:50:42.181", "messageId": "EXAMPLEdfc5f485-
d40a2543-2cac-4b84-8a8f-30bebd3820c-000000", "ses_to": "[\"success@simulator.amazonses.com
\" ]", "ses_configuration_set": "[\"MyConfigSet\" ]" }
```

Überwachung Ihrer Amazon SES Absenderzuverlässigkeit

Amazon SES verfolgt aktiv mehrere Metriken, die Ihrer Zuverlässigkeit als Absender 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](#) (p. 400)
- [Reputation Dashboard-Nachrichten](#) (p. 402)
- [Erstellen von Zuverlässigkeitsüberwachungsalarmen mit CloudWatch](#) (p. 415)
- [SNDS-Metriken für dedizierte IP-Adressen](#) (p. 418)
- [Automatisches Unterbrechen des E-Mail-Versands](#) (p. 419)

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 das Reputation Dashboard an

1. Melden Sie sich beim [anAWS Management Console](#) und öffnen Sie die Amazon 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 kurze Beschreibung des Zustands Ihres Kontos. Mögliche Werte sind:
 - **Healthy** – Es gibt derzeit keine Probleme, die sich auf Ihr Konto auswirken.

- 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— 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.
- Sendeunterbrechung— Die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrochen wurde. Während die Fähigkeit Ihres Kontos 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).
- Pending send pause— 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.
- Complaint Rate – Der Prozentsatz der von Ihrem Konto gesendeten E-Mails, die von Empfängern als Spam gemeldet wurden.

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:

- Fehlerfrei— Die Metrik befindet sich im Normalbereich.
- Fast geheilt— Aufgrund der Metrik wurde eine Prüfung für Ihr Konto festgelegt. Seit Beginn des Überprüfungszeitraums blieb die Metrik unterhalb der Höchstgrenze. Wenn die Metrik unterhalb der Höchstgrenze bleibt, ändert sich der Status dieser Metrik vor Ablauf des Überprüfungszeitraums in Healthy (Stabil).
- Wird geprüft— Aufgrund der Metrik wurde eine Prüfung für Ihr Konto festgelegt und es befindet sich weiterhin oberhalb der Höchstgrenze. Wenn das Problem, das zu einer Überschreitung der Höchstgrenze der Metrik führte, bis zum Ablauf des Überprüfungszeitraums nicht behoben wurde, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden.
- Sending pause— Aufgrund der Metrik haben wir die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrochen. Während die Fähigkeit Ihres Kontos 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).
- Pending send 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.
- Sonstige 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 Dashboard-Nachrichten \(p. 402\)](#).

Note

Das Reputation Dashboard ist für alle Benutzer verfügbar, die Zugriff auf die AWS Konsole haben. Sie können den Zugriff auf das Reputation Dashboard nicht über IAM-Richtlinien einschränken.

Reputation Dashboard-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](#) (p. 402)
- [Benachrichtigung zur Unzustellbarkeitsquote](#) (p. 403)
- [Benachrichtigung zur Beschwerdequote](#) (p. 404)
- [Benachrichtigungen zur Anti-Spam-Organisation](#) (p. 405)
- [Benachrichtigungen zu direktem Feedback](#) (p. 406)
- [Domain-Blocklist-Benachrichtigungen](#) (p. 407)
- [Benachrichtigung zur internen Überprüfung](#) (p. 408)
- [Benachrichtigung zum E-Mail-Dienstanbieter](#) (p. 410)
- [Benachrichtigung zu Empfänger-Feedback](#) (p. 411)
- [Benachrichtigung zu verknüpftem Konto](#) (p. 412)
- [Benachrichtigung zu Pseudo-E-Mail-Adressen für Spam](#) (p. 412)
- [Benachrichtigung zur Websiteanfälligkeit](#) (p. 413)
- [Sonstige Benachrichtigung](#) (p. 414)

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.
- **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**— 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.
- **Sendeunterbrechung**— Wir haben die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrochen. Während die Fähigkeit Ihres Kontos 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 prüfverfahren — Häufig gestellte Fragen](#) (p. 529).
- **Sendeunterbrechung**— 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:

- Fehlerfrei— Die Metrik befindet sich im Normalbereich.
- Fast geheilt— Aufgrund der Metrik wurde eine Prüfung für Ihr Konto festgelegt. Seit Beginn des Überprüfungszeitraums blieb die Metrik unterhalb der Höchstgrenze. Wenn die Metrik unterhalb der Höchstgrenze bleibt, ändert sich der Status dieser Metrik vor Ablauf des Überprüfungszeitraums in Healthy (Stabil).
- Wird geprüft— Aufgrund der Metrik wurde eine Prüfung für Ihr Konto festgelegt und es befindet sich weiterhin oberhalb der maximalen Rate. Wenn das Problem, das zu einer Überschreitung der Höchstgrenze der Metrik führte, bis zum Ablauf des Überprüfungszeitraums nicht behoben wurde, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden.
- Pending pause— Aufgrund der Metrik haben wir die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrochen. Während die Fähigkeit Ihres Kontos zum Senden 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).
- Sendeunterbrechung— 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

Dieser Abschnitt enthält 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 harter 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 berücksichtigt Amazon SES keine temporären Unzustellbarkeiten (die auftreten, wenn die Adresse eines Empfängers vorübergehend keine Nachrichten empfangen kann). Unzustellbare E-Mails, die Sie an verifizierte Adressen und Domänen senden, sowie von Ihnen an die [Amazon SES Postfachsimulator \(p. 198\)](#), werden auch in dieser Berechnung nicht betrachtet.

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](#) (p. 503).

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 zum Senden von E-Mails bereits angehalten wurde, melden Sie sich bei der AWS-Konsole an und navigieren Sie zum Support Center. 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 implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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 prüfverfahren — Häufig gestellte Fragen](#) (p. 529).

Wenn Sie Änderungen implementieren, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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 wurden. 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-Mails generiert werden, die Sie an die [Amazon SES Postfachsimulator](#) (p. 198) 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](#) (p. 503).

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 zum Senden von E-Mails bereits angehalten wurde, melden Sie sich bei der AWS-Konsole an und navigieren Sie zum Support Center. 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 implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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 prüfverfahren — Häufig gestellte Fragen](#) (p. 529).

Wenn Sie Änderungen umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln zum Support Center. 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 Benachrichtigungen zur Anti-Spam-Organisation, die im Amazon SES Reputation Dashboard angezeigt werden.

Warum erhalten Sie diese Benachrichtigung?

Eine namhafte Anti-Spam-Organisation hat 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 implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).

Wenn Sie Änderungen umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln zum Support Center. 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 beschwerten sich beispielsweise 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 sind, oder wenn sie zu viele Nachrichten empfangen. 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 \(p. 507\)](#) 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 Versandaktivitäten \(p. 282\)](#) beschrieben.

Wenn Ihr Konto geprüft wird

Wenn Amazon SES am Ende des Überprüfungszeitraums weiterhin eine signifikante Anzahl direkter Beschwerden über 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 implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren 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 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).

Wenn Sie Änderungen umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln zum Support Center. 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 (Domain Blocklist) 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 steht in keiner Verbindung mit Amazon SES oder 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, die für böswillige Zwecke verwendet wurden. Wenn Ihre E-Mails weiterhin eine signifikante Anzahl von Verweisen auf diese Domänen enthalten, unterbrechen wir möglicherweise die Fähigkeit Ihres Kontos, E-Mails zu senden, bis Sie das Problem beheben.

Wenn Sie Änderungen implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).

Wenn Sie Änderungen umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln zum Support Center. 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/> Wenn 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 steht in keiner Verbindung mit Amazon SES oder 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 umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln 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.

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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#) 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-Anbieter 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 implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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-Diensteanbietern 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).

Wenn Sie Änderungen umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln zum Support Center. 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 Amazon SES Unzustellbarkeits- und Beschwerdebenachrichtigungen von 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 \(p. 507\)](#) 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 Versandaktivitäten \(p. 282\)](#) 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 implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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-Dienst Anbietern 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).

Wenn Sie Änderungen umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln zum Support Center. 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 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 haben Grund zu der Annahme, dass das problematische Konto mit Ihrem AWS Konto verknüpft ist. Daher haben wir Maßnahmen eingeleitet, um ähnliche Probleme zu unterbinden.

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 implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren 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 Pending 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 Berichten zu Pending Spam (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 \(p. 507\)](#) 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 Versandaktivitäten \(p. 282\)](#) 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 implementiert haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#).

Wenn Sie Änderungen umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln zum Support Center. 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-Diensteanbietern 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 Support-Center-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 umgesetzt haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und wechseln zum Support Center. 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 prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#) 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 Support Center-Fall, den wir in Ihrem Namen geöffnet haben. Um auf das Support Center zuzugreifen, melden Sie sich bei der AWS-Konsole an und wählen Sie dann Support Center aus. 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 Zuverlässigkeitsüberwachungsalarmen mit CloudWatch

Amazon SES veröffentlicht automatisch eine Reihe von Reputationsbezogenen Metriken in 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

In den Verfahren in diesem Abschnitt werden einige Informationen zu optionalen Einstellungen für CloudWatch Alarme weggelassen. Detaillierte Anweisungen finden Sie unter [.Erstellen von Amazon CloudWatch Alarmen](#) in der Amazon CloudWatch-Benutzerhandbuchaus.

So erstellen Sie einen CloudWatch Alarm

1. Erstellen Sie ein neues 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 Themas](#) und [Abonnieren eines Themas durch einen Endpunkt](#) in der Amazon Simple Notification Service-Entwicklerhandbuchaus.
2. Öffnen Sie die CloudWatch-Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
3. Klicken Sie im Navigationsbereich auf Alarme.
4. Führen Sie auf der Seite Specify metric and conditions (Metrik und Bedingungen angeben) die folgenden Schritte aus:
 - a. Wählen Sie unter Metric (Metrik) die Option Select metric (Metrik auswählen) aus.
 - b. Wählen Sie in der Liste der Metriken SES aus.

Note

Wenn Sie noch nie eine E-Mail in der aktuellen AWS Region gesendet haben, SES wird möglicherweise nicht in der Liste der verfügbaren Metriken angezeigt. Sie können die SES-Metriken werden angezeigt, indem eine Test-E-Mail an die [Amazon SES Postfachsimulator \(p. 198\)](#) aus. Die Metriken werden in CloudWatch Metriken innerhalb weniger Minuten angezeigt.

- c. Wählen Sie Account Metrics (Konto-Metriken) aus.
- d. Wählen Sie die Metrik aus, für die Sie den Alarm erstellen möchten.

Wenn Sie zum Beispiel einen Alarm erstellen möchten, wenn die Unzustellbarkeitsquote ein bestimmtes Level erreicht hat, wählen Sie Reputation.BounceRate aus. Wenn Sie einen Alarm erstellen möchten, wenn die Beschwerdequote ein bestimmtes Level erreicht hat, wählen Sie Reputation.ComplaintRate aus.

Note

Die Reputation.Bouncerate und Ruf.Reklamation Die Metriken werden auf dieser Seite nicht angezeigt, wenn Ihr Konto noch nie eine Unzustellbarkeits- oder Beschwerde hat.

Nachdem Sie eine Metrik ausgewählt haben, wählen Sie Select metric (Metrik auswählen) aus.

- e. Wählen Sie im Abschnitt Conditions (Bedingungen) unter Threshold type (Schwellenwerttyp) die Option Static (Statisch) aus.
- f. **UND** Immer wenn die Zuverlässigkeit **MetricName** ist, wählen Sie Größer/Gleich aus.
- g. **UND** **TURN** Geben Sie den Wert an, der CloudWatch veranlassen soll, einen Alarm auszulösen.

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 CloudWatch so konfigurieren, dass Ihnen eine Benachrichtigung gesendet wird, wenn die Unzustellbarkeitsquote für Ihr Konto größer oder gleich 0,05 (5%) ist, wie in der folgenden Abbildung veranschaulicht.

Conditions

Threshold type



Static

Use a value as a threshold



An

Us

Whenever Reputation.BounceRate is...

Define the alarm condition



Greater

> threshold



Greater/Equal

>= threshold



Lo

<=

than...

Define the threshold value

0.05



Must be a number

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 CloudWatch so konfigurieren, dass Ihnen eine Benachrichtigung gesendet wird, wenn die Beschwerdequote für Ihr Konto größer oder gleich 0,001 (0,1%) ist, wie in der folgenden Abbildung veranschaulicht.

Conditions

Threshold type



Static

Use a value as a threshold



Any

Use

Whenever Reputation.ComplaintRate is...

Define the alarm condition



Greater

> threshold



Greater/Equal

>= threshold



Low

<= threshold

than...

Define the threshold value

0.001



Must be a number

- h. Wählen Sie unter Additional configuration (Zusätzliche Konfiguration) für Missing data treatment (Behandlung fehlender Daten) die Option Treat missing data as ignore (maintain the alarm state) (Fehlende Daten ignorieren (Alarmstatus beibehalten)) aus.
 - i. Wählen Sie Next.
5. Führen Sie auf der Seite Configure details (Details konfigurieren) die folgenden Schritte aus:
 - a. Wählen Sie für Whenever this alarm state is (Lautete dieser Alarmstatus) die Option in Alarm (aktiv) aus.
 - b. Wählen Sie unter Select an SNS topic (SNS-Thema auswählen) die Option Select an existing SNS topic (Vorhandenes SNS-Thema auswählen) aus. Wählen Sie für Send notification to (Benachrichtigung senden an) das Thema aus, das Sie in Schritt 1 erstellt und abonniert haben.
 - c. Wählen Sie Next.
6. Führen Sie auf der Seite Add a description (Beschreibung hinzufügen) die folgenden Schritte aus:
 - a. Geben Sie unter Alarm name (Alarmname) einen eindeutigen Namen für den Alarm ein.
 - b. (Optional) Geben Sie unter Alarm description (Beschreibung des Alarms) einen Text ein, der den Alarm beschreibt.
 - c. Wählen Sie Next.
7. Bestätigen Sie auf der Seite Preview and create (Voranzeigen und erstellen) die Einstellungen, die Sie auf den vorherigen Seiten angegeben haben. Wenn Sie bereit sind, den Alarm zu erstellen, wählen Sie Create alarm (Alarm erstellen) aus.

SNDS-Metriken für dedizierte IP-Adressen

Sie können Smart Network Data Services (SNDS) Daten für geleaste dedizierte IP-Adressen in jeder AWS Region anzeigen, in der Sie Amazon SES verwenden. Die SNDS-Daten sind über die Amazon CloudWatch Konsole verfügbar.

SNDS ist ein Outlook-Programm, mit dem IP-Besitzern Spam in ihrem IP-Bereich verhindern können. Amazon SES stellt diese wichtigen Daten für diejenigen bereit, die dedizierte IPs leasen. Die SNDS-Daten bieten Einblicke in das E-Mail-Versandverhalten der IP und rufen Bereiche auf, die für Ihre Absenderzuverlässigkeit Sorge tragen.

Note

Wenn Sie sich auf Outlook beziehen, deckt dies alle Domänen ab, die sie verfolgen. Dies kann beispielsweise Hotmail.com, Outlook.com und Live.com umfassen.

So zeigen Sie SNDS-Daten für Ihre dedizierten IP-Adressen an

1. Melden Sie sich bei der Amazon CloudWatch Konsole unter an <https://console.aws.amazon.com/cloudwatch/aus>.
2. Wählen Sie im Navigationsbereich Metrics aus.
3. Klicken Sie auf derAlle MetrikenWählen Sie in der von Ihnen gewünschten AWS RegionSESUNDERAWS-Namespacesaus.
4. Wählen Sie aus.IP-Metriken, die Ihnen alle Ihre dedizierten IPs, die von SNDS verfolgt werden, zeigt.
5. Zeigen Sie in dieser Liste alle von SNDS verfolgten dedizierten IPs an, oder wählen Sie eine einzelne IP-Adresse aus, um nur die Metriken anzuzeigen.

Die folgenden Metriken werden für jede dedizierte IP-Adresse bereitgestellt und von Outlook definiert. Weitere Informationen hierzu finden Sie unter SNDS von Outlook– [Häufig gestellte Fragen](#)aus.

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.rcptBefehle**- Dies ist die Anzahl der RCPT-Befehle, die SNDS für die spezifische IP-Adresse während des Aktivitätszeitraums wahrgenommen hat. RCPT-Befehle sind Teil des SMTP-Protokolls, das zum Senden von E-Mails verwendet wird, 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 wahrgenommen 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.messageChipients**- Die Anzahl der Empfänger von Nachrichten, die von SNDS für die spezifische IP-Adresse während des Aktivitätszeitraums wahrgenommen werden.
- **SNDS.Spamrate**- Zeigt die aggregierten Ergebnisse der Spam-Filterung an, die auf alle Nachrichten angewendet wird, die von der IP-Adresse während des angegebenen Aktivitätszeitraums gesendet wurden.
 - Eine SpamRate von 0 bedeutet, dass die IP-Adresse weniger als 10% Spam hat.
 - Eine SpamRate von 0,5 bedeutet, dass zwischen 10% und 90% Spam aus der IP-Adresse generiert wird.
 - Eine SpamRate von 1 bedeutet, dass mindestens 90% Spam von der IP-Adresse generiert werden.

- SNDS.Reklamation- Dies ist der Bruchteil der Zeit, über die eine von der IP empfangene Nachricht von einem Outlook-Benutzer während des Aktivitätszeitraums beschwert wird.
 - Eine Beschwerde von 1 bedeutet eine 100% ige Beschwerderate.
 - Eine Beschwerde von 0,05 würde beispielsweise eine Reklamationsrate von 5% bedeuten.
 - Eine Reklamation von 0 bedeutet, dass die Rate weniger als 0,1% beträgt.
- SNDS.Traphits- Zeigt die Anzahl der Nachrichten an, die an „Trap-Konten“ gesendet werden. 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.

Fragen zur Fehlersuche

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 ändern sich die SNDS.Spamrate und SNDS.Complaintrate Metriken 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 möchten Sie andere Internetdienstanbieter (ISPs) sowie Ihre Interaktionsnummern überprüfen, um sicherzustellen, dass es sich nicht um ein globales Problem handelt. Wenn es sich um ein globales Problem handelt, können Probleme mit mehreren ISPs auftreten, die ein Problem mit Listen, Inhalten, Verteilung oder Berechtigungen vorschlagen würden. Wenn es sich um Outlook handelt, lesen Sie [wie Sie am besten an Outlook liefern](#) aus. Weitere Informationen zu bewährten Methoden für finden Sie unter [Bewährte Methoden für das Versenden von Amazon SES mit \(p. 503\)](#) aus.

F3. Welche Aktionen wird AWS Support ausführen, wenn sich meine SNDS.Spamrate von einem Wert von 0 (oder 0,5) zu 1 ändert?

AWS hat keine Kontrolle über SNDS und hat daher keinen Einfluss auf SNDS. Alle Risikominderungsanforderungen müssen direkt bei Outlook über ihre [Neues Support-Anfrageformular](#) aus.

Automatisches Unterbrechen des E-Mail-Versands

Um die Zuverlässigkeit des Senders zu schützen, können Sie den E-Mail-Versand für Nachrichten, die mit bestimmten Konfigurationssätzen gesendet werden, oder für alle Nachrichten, die von Ihrem Amazon SES S-Konto in einer bestimmten AWS Region gesendet werden, vorübergehend pausieren.

Durch die Nutzung von Amazon CloudWatch und Lambda können Sie eine Lösung erstellen, die Ihren E-Mail-Versand automatisch pausiert, wenn Ihre Zuverlässigkeitsmetriken (wie z. B. Unzustellbarkeitsquote oder Beschwerdequote) bestimmte Grenzwerte 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 \(p. 420\)](#)
- [Automatisches Pausieren des E-Mail-Versands für einen Konfigurationssatz \(p. 424\)](#)

Automatisches Pausieren des E-Mail-Versands für Ihr gesamtes Amazon SES Konto

Die Verfahren in diesem Abschnitt erläutern die Schritte zum Einrichten von Amazon SES, Amazon SNS, Amazon CloudWatch und AWS Lambda, um das Senden von E-Mails für Ihr Amazon SES S-Konto in einer einzelnen AWS Region automatisch zu pausieren. 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 \(p. 420\)](#)
- [Teil 2: Erstellen der Lambda -Funktion \(p. 420\)](#)
- [Teil 3: Erneutes Aktivieren des E-Mail-Versands für Ihr Konto \(p. 422\)](#)
- [Teil 4: Erstellen eines Amazon SNS -Themas \(p. 422\)](#)
- [Teil 5: Erstellen eines CloudWatch Alarms \(p. 423\)](#)
- [Teil 6: Testen der Lösung \(p. 424\)](#)

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 `UpdateAccountSendingEnabledAPI`-Operation.

So erstellen Sie die IAM-Rolle

1. Öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.
2. Wählen Sie im Navigationsbereich Roles aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie unter Select type of trusted entity die Option AWS service aus.
5. Wählen Sie unter Choose the service that will use this role die Option Lambda aus. Wählen Sie Weiter. Berechtigungen.
6. Wählen Sie auf der Seite Attach permissions policies die folgenden Richtlinien aus:
 - `AWSLambdaBasicExecutionRole`
 - `AmazonSESFullAccess`

Tip

Verwenden Sie das Suchfeld oben in der Liste der Richtlinien, um diese Richtlinien schnell zu finden.

Wählen Sie Weiter. Prüfen.

7. Geben Sie auf der Seite Review im Feld Name einen Namen für die Rolle ein. Wählen Sie 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 AWS Lambda-Konsole <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 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 die Option Author from scratch.
5. Führen Sie unter Author from scratch die folgenden Schritte durch:
 - Für Name Geben Sie unter Verwendung eines Namens für die Lambda -Funktion ein.
 - Wählen Sie in Runtime (Laufzeit) Node.js 6.10 (Node.js 6.10) aus.
 - Wählen Sie für Role die Option Choose an existing role.
 - Für Vorhandene Rolle Wählen Sie die IAM-Rolle aus, die Sie in [the section called "Teil 1: Erstellen einer IAM-Rolle" \(p. 420\)](#).

Wählen Sie Create function (Funktion erstellen).

6. Fügen Sie sie im Code-Editor unter Function code (Funktionscode) den folgenden Code ein:

```
'use strict';

var aws = require('aws-sdk');

// Create a new SES object.
var ses = new aws.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 Save (Speichern) aus.

7. Wählen Sie Test aus. Wenn das Fenster Configure test event angezeigt wird, geben Sie einen Namen im Feld Event name ein und wählen Sie dann Create 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:

- Stellen Sie sicher, dass die IAM-Rolle, die Sie in [the section called “Teil 1: Erstellen einer IAM-Rolle” \(p. 420\)](#) enthält die richtigen Richtlinien.
- Stellen Sie sicher, 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 beim Testen der Lambda Funktion in [the section called “Teil 2: Erstellen der Lambda -Funktion” \(p. 420\)](#) Vergewissern Sie sich, dass das Senden von E-Mails für Ihr Amazon SES Konto pausiert ist. In den meisten Fällen sollten Sie den Versand für Ihr Konto erst anhalten, wenn 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: `aws ses update-account-sending-enabled --enabled --region us-west-2`

Note

Ersetzen Sie **us-west-2** im vorangehenden Befehl durch den Namen der Region, in der Sie den E-Mail-Versand wieder aktivieren möchten.

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 us-west-2`

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

Damit CloudWatch Ihre Lambda Funktion ausführt, wenn ein Alarm ausgelöst wird, müssen Sie zuerst ein Amazon SNS -Thema erstellen und es für die Lambda -Funktion abonnieren.

So erstellen Sie das Amazon SNS -Thema

1. Öffnen Sie die Amazon 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 aus.
4. Wählen Sie Create new topic.
5. Geben Sie im Fenster Create new topic unter Topic name einen Namen für das Thema ein. Optional können Sie im Feld Display name einen aussagekräftigeren Namen eingeben.

Wählen Sie Create topic aus.

6. Aktivieren Sie in der Liste der Themen das Kontrollkästchen neben dem im vorherigen Schritt erstellten Thema. Wählen Sie im Menü Actions die Option Subscribe to topic aus.

7. Wählen Sie im Fenster Create subscription folgende Optionen aus:
 - Wählen Sie unter Protocol die Option AWS Lambda aus.
 - Für-Endpunkt die Lambda Funktion aus, die Sie in [the section called “Teil 2: Erstellen der Lambda -Funktion” \(p. 420\)](#).
 - Wählen Sie für Version or alias die Option default aus.
8. Wählen Sie Create subscription.

Teil 5: Erstellen eines CloudWatch Alarms

Dieser Abschnitt enthält Verfahren zum Erstellen eines Alarms in CloudWatch, der ausgelöst wird, wenn eine Metrik einen bestimmten Schwellenwert erreicht. Wenn der Alarm ausgelöst wird, übermittelt er eine Benachrichtigung an das Amazon SNS -Thema, das Sie in [the section called “Teil 4: Erstellen eines Amazon SNS -Themas” \(p. 422\)](#), die dann die Lambda Funktion ausführt, die Sie in [the section called “Teil 2: Erstellen der Lambda -Funktion” \(p. 420\)](#).

So erstellen Sie einen CloudWatch-Alarm

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 Alarme.
4. Wählen Sie Create Alarm aus.
5. Wählen Sie im Fenster Create Alarm unter SES Metrics die Option Account Metrics aus.
6. Wählen Sie unter Metric Name eine der folgenden Optionen aus:
 - Reputation.BounceRate – Wählen Sie diese Metrik aus, wenn Sie das Senden von E-Mails für Ihr Konto pausieren möchten, sobald die Quote der permanent unzustellbaren E-Mails für Ihr Konto einen von Ihnen definierten Schwellenwert überschreitet.
 - Reputation.ComplaintRate – Wählen Sie diese Metrik aus, wenn Sie das Senden von E-Mails für Ihr Konto pausieren möchten, sobald die Beschwerdequote für Ihr Konto einen von Ihnen definierten Schwellenwert überschreitet.

Wählen Sie Next.

7. Führen Sie folgende Schritte aus:
 - Geben Sie unter Alarm Threshold im Feld Name einen Namen für den Alarm ein.
 - UNDERWENEVER Reputation.Bouncerate oder .WENEVER Ruf.Reklamation Geben Sie unter den Schwellenwert an, der zum Auslösen des Alarms führt.

Note

Für Ihr Konto wird automatisch eine Prüfung festgelegt, wenn Ihre Unzustellbarkeitsquote 10 % überschreitet oder wenn Ihre Beschwerdequote 0,5 % überschreitet. Wenn Sie die Unzustellbarkeits- und Beschwerdequote angeben, die dazu führt, dass der CloudWatch Alarm ausgelöst wird, empfehlen wir, Werte zu verwenden, die unterhalb dieser Quoten liegen, um zu verhindern, dass eine Prüfung für Ihr Konto festgelegt wird.

- Wählen Sie unter Actions für Whenever this alarm die Option State is ALARM aus. 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” \(p. 422\)](#).

Wählen Sie Create Alarm aus.

Teil 6: Testen der Lösung

Sie können jetzt den Alarm testen, um sicherzustellen, dass er die Lambda -Funktion ausführt, wenn er in den `ALARM` Zustand. 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: `aws ses get-account-sending-enabled --region us-west-2`

Note

Ersetzen Sie `us-west-2` im vorangehenden Befehl durch den Namen der Region, die im vorherigen Schritt angegeben wurde.

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 us-west-2`

Ersetzen Sie `MyAlarm` im voranstehenden Befehl durch den Namen des Alarms, den Sie in [the section called "Teil 5: Erstellen eines CloudWatch Alarms"](#) (p. 423) erstellt haben, und geben Sie anstelle von `us-west-2` die Region ein, in der Sie den E-Mail-Versand automatisch pausieren möchten.

Note

Wenn Sie diesen Befehl ausführen, wechselt der Status des Alarms innerhalb weniger Sekunden von `OK` zu `ALARM` und zurück zu `OK`. Die Anzeige dieser Statusänderungen erfolgt auf der Registerkarte Verlauf in der CloudWatch Konsole oder mithilfe der `DescribeAlarmHistory`.

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 us-west-2`

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"](#) (p. 422) 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 konfigurieren, um Zuverlässigkeitsmetriken zu exportieren, die für E-Mails gelten, die unter Verwendung eines bestimmten Konfigurationssatzes an Amazon CloudWatch gesendet werden. Anschließend können Sie diese Metriken verwenden, um CloudWatch Alarmer zu erstellen, die für diese Konfigurationssätze gelten. Wenn diese Alarmer 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 pausiert das Senden von E-Mails 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: Konfigurieren Sie die Berichterstattung von Reputation-Metriken für den Konfigurations \(p. 425\)](#)
- [Teil 2: Erstellen einer IAM-Rolle \(p. 425\)](#)
- [Teil 3: Erstellen der Lambda -Funktion \(p. 426\)](#)
- [Teil 4: Erneutes Aktivieren des E-Mail-Versands für den Konfigurationssatz \(p. 427\)](#)
- [Teil 5: Erstellen eines Amazon SNS -Themas \(p. 428\)](#)
- [Teil 6: Erstellen eines CloudWatch Alarms \(p. 428\)](#)
- [Teil 7: Testen der Lösung \(p. 429\)](#)

Teil 1: Konfigurieren Sie die Berichterstattung von Reputation-Metriken für den Konfigurations

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 "Exportieren von Zuverlässigkeitsmet" \(p. 280\)](#) 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 `UpdateConfigurationSetSendingEnabledAPI-Operation`.

So erstellen Sie die IAM-Rolle

1. Öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.
2. Wählen Sie im Navigationsbereich Roles aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie unter Select type of trusted entity die Option AWS service aus.
5. Wählen Sie unter Choose the service that will use this role die Option Lambda aus. Wählen Sie Weiter. Berechtigungen.
6. Wählen Sie auf der Seite Attach permissions policies die folgenden Richtlinien aus:
 - AWS LambdaBasicExecutionRole
 - AmazonSESFullAccess

Tip

Verwenden Sie das Suchfeld oben in der Liste der Richtlinien, um diese Richtlinien schnell zu finden.

Wählen Sie Weiter. Prüfen.

7. Geben Sie auf der Seite Review 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 AWS Lambda-Konsole <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 die Option Author from scratch.
5. Führen Sie unter Author from scratch die folgenden Schritte durch:
 - Für Name Geben Sie unter Verwendung eines Namens für die Lambda -Funktion ein.
 - Wählen Sie in Runtime (Laufzeit) Node.js 6.10 (Node.js 6.10) aus.
 - Wählen Sie für Role die Option Choose an existing role.
 - Für Vorhandene Rolle Wählen Sie die IAM-Rolle aus, die Sie in [the section called “Teil 2: Erstellen einer IAM-Rolle” \(p. 425\)](#).

Wählen Sie Create function (Funktion erstellen).

6. Fügen Sie sie im Code-Editor unter Function code (Funktionscode) den folgenden Code ein:

```
'use strict';

var aws = require('aws-sdk');

// Create a new SES object.
var ses = new aws.SES();

// Specify the parameters for this operation. In this example, you pass the
// Enabled parameter, with a value of false (Enabled = false disables email
// sending, Enabled = true enables it). You also pass the ConfigurationSetName
// parameter, with a value equal to the name of the configuration set for
// which you want to pause email sending.
var params = {
  ConfigurationSetName: 'ConfigSet',
  Enabled: false
};

exports.handler = (event, context, callback) => {
  // Pause sending for a configuration set
  ses.updateConfigurationSetSendingEnabled(params, function(err, data) {
    if(err) {
```

```
        console.log(err.message);  
    } else {  
        console.log(data);  
    }  
    });  
};
```

Ersetzen Sie **ConfigSet** im vorherigen Code mit dem Namen des Konfigurationssatzes. Wählen Sie Save (Speichern) aus.

- Wählen Sie Test aus. Wenn das Fenster Configure test event angezeigt wird, geben Sie einen Namen im Feld Event name ein und wählen Sie dann Create aus.
- Stellen Sie sicher, dass die Benachrichtigungsleiste oben auf der Seite **Execution result**: succeeded angezeigt. Wenn die Funktion nicht ausgeführt werden kann, führen Sie die folgenden Schritte aus:
 - Stellen Sie sicher, dass die IAM-Rolle, die Sie in [the section called "Teil 2: Erstellen einer IAM-Rolle"](#) (p. 425) enthält die richtigen Richtlinien.
 - Stellen Sie sicher, dass der Code in der Lambda -Funktion keine Syntaxfehler enthält. Der Lambda -Code-Editor hebt automatisch Syntaxfehler und andere potenzielle Probleme hervor.

Teil 4: Erneutes Aktivieren des E-Mail-Versands für den Konfigurationssatz

Ein Nebeneffekt beim Testen der Lambda Funktion in [the section called "Teil 3: Erstellen der Lambda -Funktion"](#) (p. 426) Teil davon, dass das Senden von E-Mails für den Konfigurationssatz angehalten wird. In den meisten Fällen sollten Sie den Versand für den Konfigurationssatz erst anhalten, wenn 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

- 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 im voranstehenden Befehl **ConfigSet** durch den Namen des Konfigurationssatzes, für den Sie den E-Mail-Versand pausieren möchten, und geben Sie anstelle von **us-west-2** die Region ein, in der Sie den E-Mail-Versand automatisch pausieren möchten.

- 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

Damit CloudWatch die Lambda Funktion ausführt, wenn ein Alarm ausgelöst wird, müssen Sie zuerst ein Amazon SNS -Thema erstellen und es für die Lambda -Funktion abonnieren.

So erstellen Sie das Amazon SNS -Thema

1. Öffnen Sie die Amazon 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 aus.
4. Wählen Sie Create new topic.
5. Geben Sie im Fenster Create new topic unter Topic name einen Namen für das Thema ein. Optional können Sie im Feld Display name einen aussagekräftigeren Namen eingeben.

Wählen Sie Create topic aus.

6. Aktivieren Sie in der Liste der Themen das Kontrollkästchen neben dem im vorherigen Schritt erstellten Thema. Wählen Sie im Menü Actions die Option Subscribe to topic aus.
7. Wählen Sie im Fenster Create subscription folgende Optionen aus:
 - Wählen Sie unter Protocol die Option AWS Lambda aus.
 - Für-Endpunkt die Lambda Funktion aus, die Sie in [the section called "Teil 3: Erstellen der Lambda -Funktion" \(p. 426\)](#).
 - Wählen Sie für Version or alias die Option default aus.
8. Wählen Sie Create subscription.

Teil 6: Erstellen eines CloudWatch Alarms

Dieser Abschnitt enthält Verfahren zum Erstellen eines Alarms in CloudWatch, der ausgelöst wird, wenn eine Metrik einen bestimmten Schwellenwert erreicht. Wenn der Alarm ausgelöst wird, übermittelt er eine Benachrichtigung an das Amazon SNS -Thema, das Sie in [the section called "Teil 5: Erstellen eines Amazon SNS -Themas" \(p. 428\)](#), die dann die Lambda Funktion ausführt, die Sie in [the section called "Teil 3: Erstellen der Lambda -Funktion" \(p. 426\)](#).

So erstellen Sie einen CloudWatch-Alarm

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 aus.
4. Wählen Sie Create Alarm aus.

5. Wählen Sie im Fenster Create Alarm unter SES Metrics die Option Configuration Set Metrics aus.
6. Suchen Sie in der ses:configuration-set-Spalte den Konfigurationssatz, für den Sie einen Alarm erstellen möchten. Wählen Sie unter Metric Name eine der folgenden Optionen aus:

- Reputation.BounceRate – Wählen Sie diese Metrik aus, wenn Sie das Senden von E-Mails für den Konfigurationssatz pausieren möchten, sobald die gesamte Unzustellbarkeitsquote für den Konfigurationssatz einen von Ihnen definierten Schwellenwert überschreitet.
- Reputation.ComplaintRate – Wählen Sie diese Metrik aus, wenn Sie das Senden von E-Mails für den Konfigurationssatz pausieren möchten, sobald die gesamte Beschwerdequote für den Konfigurationssatz einen von Ihnen definierten Schwellenwert überschreitet.

Wählen Sie Next.

7. Führen Sie folgende Schritte aus:

- Geben Sie unter Alarm Threshold im Feld Name einen Namen für den Alarm ein.
- UNDERWENEVER Reputation.Bouncerateoder .WENEVER Ruf.ReklamationGeben Sie unter den Schwellenwert an, der zum Auslösen des Alarms führt.

Note

Wenn die gesamte Unzustellbarkeitsquote für Ihr Amazon SES S-Konto 10% überschreitet, oder wenn die gesamte Beschwerdequote für Ihr Amazon SES-Konto 0,5% überschreitet, wird Ihr Amazon SES-Konto automatisch geprüft. Wenn Sie die Unzustellbarkeits- und Beschwerdequote angeben, die dazu führt, dass der CloudWatch Alarm ausgelöst wird, empfehlen wir, Werte zu verwenden, die weit unterhalb dieser Quoten liegen, um zu verhindern, dass eine Prüfung für Ihr Konto festgelegt wird.

- Wählen Sie unter Actionsfür Whenever this alarm die Option State is ALARM aus. FürSend notification to (Benachrichtigung senden an)das Amazon SNS -Thema aus, das Sie inthe section called "Teil 5: Erstellen eines Amazon SNS -Themas" (p. 428).

Wählen Sie Create Alarm aus.

Teil 7: Testen der Lösung

Sie können jetzt den Alarm testen, um sicherzustellen, dass er die Lambda -Funktion ausführt, wenn er in dieALARMZustand. Sie können dasSetAlarmStateVerwenden Sie die CloudWatch API, um den Status des Alarms temporär 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 --region us-west-2`

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* im vorherigen Befehl mit dem Namen des Alarms, den Sie in [the section called "Teil 6: Erstellen eines CloudWatch Alarms" \(p. 428\)](#) erstellt haben.

Note

Wenn Sie diesen Befehl ausführen, wechselt der Status des Alarms innerhalb weniger Sekunden von `OK` zu `ALARM` und zurück zu `OK`. Die Anzeige dieser Statusänderungen erfolgt auf der Registerkarte `Verlauf` in der CloudWatch Konsole oder mithilfe der `DescribeAlarmHistory`.

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 Wert von `SendingEnabled` ist `false` Wählen Sie aus, 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: Erneutes Aktivieren des E-Mail-Versands für den Konfigurationssatz" \(p. 427\)](#) aus, um den E-Mail-Versand für den Konfigurationssatz erneut zu aktivieren.

Steuern des Zugriffs auf Amazon SES

Sie können die AWS Identity and Access Management (IAM) mit Amazon Simple Email Service (Amazon SES) angeben, welche Amazon SES-API-Aktionen ein IAM-Benutzer, eine IAM-Gruppe oder eine IAM-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 Amazon 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 weisen die Richtlinie einem Benutzer zu. Informationen zum Erstellen von IAM-Richtlinien finden Sie unter [IAM-Benutzerhandbuch](#). Abgesehen vom Anwenden der Einschränkungen, die Sie in Ihrer Richtlinie festlegen, gibt es keine Änderungen daran, wie Benutzer mit Amazon SES interagieren oder darin, wie Amazon SES Anfragen ausführt.

Note

Sie können auch mithilfe der Sendeautorisierungsrichtlinien den Zugriff auf Amazon SES steuern. Während IAM-Richtlinien regeln, welche Aufgaben einzelne IAM-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](#) (p. 162).

Wenn Sie nach Informationen zum Generieren von Amazon SES Anmeldeinformationen für einen vorhandenen IAM-Benutzer suchen, lesen Sie nach unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen](#) (p. 95).

Erstellen von IAM-Richtlinien für den Zugriff auf Amazon SES

In diesem Abschnitt wird erklärt, wie Sie IAM-Richtlinien speziell mit Amazon SES verwenden können. Informationen zum Erstellen von IAM-Richtlinien im Allgemeinen finden Sie unter [IAM-Benutzerhandbuch](#).

Es gibt drei Gründe, warum Sie möglicherweise IAM mit Amazon SES verwenden möchten:

- 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 steuern, wie den Zeitraum, in dem ein Benutzer die APIs aufrufen darf, zu deren Verwendung er autorisiert ist.

Beschränken der Aktion

Um zu steuern, welche Amazon SES Aktionen ein Benutzer durchführen kann, verwenden Sie die `ActionElement` einer IAM-Richtlinie. Sie können die `Action`-Element auf eine beliebige Amazon SES API-Aktion festlegen, indem Sie dem API-Namen die kleingeschriebene Zeichenfolge voranstellen: `ses:`. 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:

Wenn das Symbol **`Action`**-Element erlaubt nur den Zugriff auf -APIs für den E-Mail-Versand (d. h. `ses:SendEmail` und/oder `ses:SendRawEmail`):

- Um dem Benutzer das Senden von jeder Identität in Ihrem AWS-Konto zu erlauben, setzen Sie `Resource` auf `*`.
- Um die Identitäten einzuschränken, von denen ein Benutzer senden darf, legen Sie `Resource` auf die ARNs der Identitäten fest, deren Verwendung Sie dem Benutzer gestatten.

Wenn das Symbol **`Action`**-Element ermöglicht den Zugriff auf alle 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:
 - Eine, in der `Action` auf eine explizite Liste der erlaubten APIs festgelegt ist, die keine E-Mails senden, und `Resource` auf `*` gesetzt ist.
 - Eine, in der `Action` auf eine der APIs festgelegt ist, die E-Mails senden (`ses:SendEmail` und/oder `ses:SendRawEmail`), und `Resource` auf den/die ARN(s) der Identitäten gesetzt ist, die die Benutzer verwenden dürfen.

Für eine Liste der verfügbaren Amazon SES Aktionen siehe die [Amazon Simple Email Service API-Referenz](#) und [Verweis auf Amazon Simple Email Service API-Version 2](#). Wenn der IAM-Benutzer die SMTP-Schnittstelle verwenden möchte, müssen Sie den Zugriff auf `ses:SendRawEmail` auf ein Minimum.

Beschränken von E-Mail-Adressen

Wenn Sie den Benutzer auf bestimmte E-Mail-Adressen beschränken möchten, können Sie einen `Condition`-Block verwenden. In der `Condition`-Block geben Sie Bedingungen mithilfe von Bedingungsschlüsseln an, wie im [IAM-Benutzerhandbuch](#). Durch die Nutzung von Bedingungsschlüsseln können Sie die folgenden E-Mail-Adressen steuern:

Note

Diese Bedingungsschlüssel für E-Mail-Adressen gelten nur für die APIs in der folgenden Tabelle.

Bedingungsschlüssel	Beschreibung	API
<code>ses:Recipients</code>	Beschränkt die Empfängeradressen,	<code>SendEmail</code> , <code>SendRawEmail</code>

Bedingungsschlüssel	Beschreibung	API
	einschließlich der Adressen "To", "CC" und "BCC".	
<code>ses:FromAddress</code>	Beschränkt die "From"-Adresse.	<code>SendEmail</code> , <code>SendRawEmail</code> , <code>SendBounce</code>
<code>ses:FromDisplayName</code>	Beschränkt die "From"-Adresse, die als Anzeigename verwendet wird.	<code>SendEmail</code> , <code>SendRawEmail</code>
<code>ses:FeedbackAddress</code>	Beschränkt die "Return-Path"-Adresse. Dies ist die Adresse, an die Unzustellbarkeitsnachrichten und Beschwerden an Sie anhand von Feedback-E-Mails weitergeleitet werden können. Weitere Informationen zum Weiterleiten von Feedback per E-Mail finden Sie unter Per E-Mail gesendete Amazon SES S-Benachrichtigungen (p. 289).	<code>SendEmail</code> , <code>SendRawEmail</code>

Beschränken der allgemeinen API-Nutzung

Durch die Verwendung von AWS-weiten Schlüsseln in Bedingungen können Sie den Zugriff auf Amazon SES basierend auf Aspekten beschränken, wie z. B. das Datum und die Uhrzeit, zu dem Benutzer auf APIs zugreifen kann. Amazon SES implementiert nur die folgenden AWS-weiten Richtlinienschlüssel:

- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:UserAgent`

Weitere Informationen zu diesen Schlüsseln finden Sie unter [IAM-Benutzerhandbuch](#).

Beispielrichtlinien für Amazon SES

In diesem Thema finden Sie Beispiele für Richtlinien, die einen Benutzerzugriff auf Amazon SES ermöglichen, jedoch nur unter bestimmten Bedingungen.

Richtlinienbeispiele in diesem Abschnitt:

- [Berechtigten von Vollzugriff auf alle Amazon SES Aktionen](#) (p. 434)
- [Erlauben von Zugriff nur auf Aktionen für den E-Mail-Versand](#) (p. 434)
- [Beschränken des Sendezeitraums](#) (p. 434)
- [Beschränken der Empfängeradressen](#) (p. 435)
- [Beschränken der "From"-Adresse](#) (p. 435)
- [Beschränken des Anzeigenamens des E-Mail-Absenders](#) (p. 436)
- [Beschränken der Zieladresse des Unzustellbarkeits- und Beschwerde-Feedbacks](#) (p. 436)

Berechtigten von Vollzugriff auf alle Amazon SES Aktionen

Mit der folgenden Richtlinie kann ein Benutzer jede beliebige Amazon SES Aktion aufrufen.

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

Erlauben von Zugriff nur auf Aktionen für den E-Mail-Versand

Mit der folgenden Richtlinie kann ein Benutzer E-Mails mithilfe von Amazon SES senden, aber keine administrativen Aktionen durchführen, wie z. B. den Zugriff auf Amazon SES-Sendestatistiken.

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

Beschränken des Sendezeitraums

Mit der folgenden Richtlinie kann ein Benutzer Amazon SES S-APIs für den E-Mail-Versand nur im Monat September 2018 aufrufen.

```
{
  "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

Mit der folgenden Richtlinie kann ein Benutzer die Amazon SES APIs für den E-Mail-Versand aufrufen, aber nur an Empfängeradressen in der Domäneexample.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource": "*",
      "Condition":{"
        "ForAllValues:StringLike":{"
          "ses:Recipients":[
            "**@example.com"
          ]
        }
      }
    }
  ]
}
```

Beschränken der "From"-Adresse

Mit der folgenden Richtlinie kann ein Benutzer die Amazon SES S-APIs für den E-Mail-Versand aufrufen, aber nur, wenn die „From“-Adresse marketing@example.com lautet.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource": "*",
      "Condition":{"
        "StringEquals":{"
          "ses:FromAddress":"marketing@example.com"
        }
      }
    }
  ]
}
```

Mit der folgenden Richtlinie kann ein Benutzer die [SendBounce](#)-API aufrufen, aber nur, wenn die „From“-Adresse bounce@example.com lautet.

```
{
  "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

Mit der folgenden Richtlinie kann ein Benutzer die Amazon SES S-APIs für den E-Mail-Versand aufrufen, aber nur, wenn der Anzeigename der „From“-Adresse Marketing.

```
{
  "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

Mit der folgenden Richtlinie kann ein Benutzer die Amazon SES S-APIs für den E-Mail-Versand aufrufen, aber nur, wenn der „Return-Path“ der E-Mail auf feedback@example.com.

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

```

```
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ses:FeedbackAddress": "feedback@example.com"
      }
    }
  ]
}
```

Protokollieren Amazon SES Aufrufen mit AWS CloudTrail

Amazon SES ist in AWS CloudTrail, einem Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in Amazon SES protokolliert. CloudTrail erfasst alle API-Aufrufe für Amazon SES als Ereignisse. Die erfassten Aufrufe umfassen Aufrufe von Amazon SES Konsole und Code-Aufrufe der Amazon SES-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Lieferung von CloudTrail-Ereignissen an einen Amazon S3 Bucket aktivieren, einschließlich Ereignissen für Amazon SES. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen. Mit den von CloudTrail erfassten Informationen können Sie die an Amazon SES gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Empfänger der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen über CloudTrail, einschließlich Konfiguration und Aktivierung, finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Amazon SES Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Wenn in Amazon SES eine unterstützte Aktivität auftritt, wird diese Aktivität in einem CloudTrail-Ereignis zusammen mit anderen AWS-Serviceereignissen in Ereignisverlauf des Benutzers. Sie können die neuesten Ereignisse in Ihrem AWS-Konto anzeigen, durchsuchen und dorthin herunterladen. Weitere Informationen finden Sie unter [Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf](#).

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich Ereignissen für Amazon SES, einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon S3-Bucket bereitzustellen. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem Amazon S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- [Übersicht zum Erstellen eines Pfads](#)
- [Siehe Von CloudTrail unterstützte Dienste und Integrationen.](#)
- [Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten](#)

Amazon SES unterstützt die Protokollierung der folgenden Aktionen als Ereignisse in CloudTrail - Protokolldateien:

- [CloneReceiptRuleSet](#)
- [CreateReceiptFilter](#)
- [CreateReceiptRule](#)
- [CreateReceiptRuleSet](#)
- [DeleteIdentity](#)
- [DeleteIdentityPolicy](#)

- [DeleteReceiptFilter](#)
- [DeleteReceiptRule](#)
- [DeleteReceiptRuleSet](#)
- [DeleteVerifiedEmailAddress](#)
- [DescribeActiveReceiptRuleSet](#)
- [DescribeReceiptRule](#)
- [DescribeReceiptRuleSet](#)
- [GetIdentityDkimAttributes](#)
- [GetIdentityNotificationAttributes](#)
- [GetIdentityPolicies](#)
- [GetIdentityVerificationAttributes](#)
- [GetSendQuota](#)
- [GetSendStatistics](#)
- [ListIdentities](#)
- [ListIdentityPolicies](#)
- [ListReceiptFilters](#)
- [ListReceiptRuleSets](#)
- [ListVerifiedEmailAddresses](#)
- [PutIdentityPolicy](#)
- [ReorderReceiptRuleSet](#)
- [SetActiveReceiptRuleSet](#)
- [SetReceiptRulePosition](#)
- [SetIdentityDkimEnabled](#)
- [SetIdentityFeedbackForwardingEnabled](#)
- [SetIdentityHeadersInNotificationsEnabled](#)
- [SetIdentityNotificationTopic](#)
- [UpdateReceiptRule](#)
- [VerifyDomainDkim](#)
- [VerifyDomainIdentity](#)
- [VerifyEmailAddress](#)
- [VerifyEmailIdentity](#)

Note

Amazon SES liefert Management-Ereignisse an CloudTrail. Verwaltungereignisse umfassen Aktionen, die im Zusammenhang mit dem Erstellen und Verwalten von Ressourcen in Ihrem AWS Konto stehen. Verwaltungereignisse umfassen Aktionen, wie z. B. Erstellen und Löschen von Identitäten oder Empfangsregeln.

Verwaltungereignisse unterscheiden sich von Datenereignissen. Datenereignisse sind Ereignisse, die im Zusammenhang mit dem Zugriff auf und der Interaktion mit Daten in Ihrem AWS Konto stehen. In Amazon SES umfassen Datenereignisse Aktionen, wie z. B. das Senden von E-Mails.

Da Amazon SES nur Verwaltungereignisse an CloudTrail liefert, werden die folgenden Ereignisse nicht aufgenommen in CloudTrail:

- [SendEmail](#)
- [SendRawEmail](#)
- [SendTemplatedEmail](#)

- `SendBulkTemplatedEmail`
- `SendCustomVerificationEmail`

Sie können die Ereignisveröffentlichung verwenden, um Ereignisse im Zusammenhang mit dem E-Mails-Versand aufzuzeichnen. Weitere Informationen finden Sie unter [Überwachen des E-Mail-Versands mit Amazon SES Ereignisveröffentlichung](#) (p. 313).

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter dem [CloudTrail `userIdentity`-Element](#).

Beispiel: Amazon SES Protokolldateieinträge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt den CloudTrail -Protokolleintrag, der die `DeleteIdentity` und `VerifyEmailIdentity`-Aktionen.

```
{
  "Records": [
    {
      "awsRegion": "us-west-2",
      "eventID": "Offa308d-1467-4259-8be3-c749753be325",
      "eventName": "DeleteIdentity",
      "eventSource": "ses.amazonaws.com",
      "eventTime": "2018-02-02T21:34:50Z",
      "eventType": "AwsApiCall",
      "eventVersion": "1.02",
      "recipientAccountId": "111122223333",
      "requestID": "50b87bfe-ab23-11e4-9106-5b36376f9d12",
      "requestParameters": {
        "identity": "amazon.com"
      },
      "responseElements": null,
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-sdk-java/unknown-version",
      "userIdentity": {
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "accountId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "principalId": "111122223333",
        "type": "Root"
      }
    },
  ],
}
```



```
"awsRegion":"us-west-2",
"eventID":"5613b0ff-d6c6-4526-9b53-a603a9231725",
"eventName":"VerifyEmailIdentity",
"eventSource":"ses.amazonaws.com",
"eventTime":"2018-02-04T01:05:33Z",
"eventType":"AwsApiCall",
"eventVersion":"1.02",
"recipientAccountId":"111122223333",
"requestID":"eb2ff803-ac09-11e4-8ff5-a56a3119e253",
"requestParameters":{"
  "emailAddress":"sender@example.com"
},
"responseElements":null,
"sourceIPAddress":"192.0.2.0",
"userAgent":"aws-sdk-java/unknown-version",
"userIdentity":{"
  "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
  "accountId":"111122223333",
  "arn":"arn:aws:iam::111122223333:root",
  "principalId":"111122223333",
  "type":"Root"
}
}
]
```

Verwenden der Amazon SES API

Sie können auf die Amazon SES API mit einem [AWS -SDK](#) Die Funktionen der Amazon SES S-API auf niedriger Ebene mit Datentypen und Funktionsaufrufen der höheren Ebene kombiniert, sodass Sie sich nicht um Details kümmern müssen. Sie können auch HTTPS-Anfragen an die Amazon SES S-API senden. Weitere Informationen zu einzelnen API-Operationen finden Sie unter [Amazon Simple Email Service API-Referenz](#) aus.

In diesem Abschnitt werden folgende Themen beschrieben:

- [Amazon SES Anforderungen](#) (p. 442)
- [Authentifizieren von Anforderungen an die Amazon SES API](#) (p. 444)
- [GET- und POST-Beispiele für die -API](#) (p. 446)
- [Amazon SES -API-Antworten](#) (p. 447)
- [Von der Amazon SES API zurückgegebene Fehlercodes](#) (p. 448)

Amazon SES Anforderungen

Sie können die Amazon SES -API direkt aufrufen, indem Sie Anforderungen an einen Amazon SES-Endpunkt stellen. Anfragen an die Amazon SES S-API sind einfache HTTPS-Anfragen, die die GET- oder die POST-Methode nutzen. API-Anforderungen müssen einen `Action`-Parameter enthalten, der die auszuführende Aktion angibt.

Important

Amazon SES unterstützt keine HTTP-Anfragen. Sie müssen stattdessen HTTPS verwenden.

Struktur einer GET-Anforderung

Dieser Leitfaden stellt die Amazon SES GET-Anfragen als URLs dar. Jede URL besteht aus den folgenden Elementen:

- Endpunkt —Die Ressource, für die die Anfrage ausgeführt wird. Eine Liste der Endpunkt-URLs für die AWS Regionen, in denen Amazon SES verfügbar ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) in der Allgemeine AWS-Referenz aus.
- Aktion – Die Aktion, die Sie auf einem Endpunkt durchführen möchten, z. B. das Senden einer Nachricht.
- Parameter – Beliebige Anforderungsparameter.

Im Folgenden finden Sie ein Beispiel für eine GET-Anfrage zum Senden einer Nachricht über den Amazon SES Endpunkt in der Region USA West (Oregon).

```
https://email.us-west-2.amazonaws.com?Action=SendEmail&Source=user%40example.com&Destination.ToAddresses.member.1=allan%40example.com&Message.Subject.Data=This%20is%20the%20subject%20line.&Message.Body.Text.Data=Hello.%20I%20hope%20you%20are%20having%20a%20good%20day.
```

Important

Da es sich bei den GET-Anfragen um URLs handelt, müssen Sie für die Parameterwerte eine URL-Codierung durchführen. In der vorherigen Beispielanforderung lautet der Wert für den `Source`-Parameter tatsächlich `user@example.com`. Da jedoch `@`-Zeichen in URLs nicht zulässig sind, wird jedes `@` in der URL als `%40` codiert.

Zur Optimierung der Lesbarkeit werden die GET-Beispiele im folgenden Format präsentiert.

```
https://email.us-west-2.amazonaws.com
?Action=SendEmail
&Source=user%40example.com
&Destination.ToAddresses.member.1=allan%40example.com
&Message.Subject.Data=This%20is%20the%20subject%20line.
&Message.Body.Text.Data=Hello.%20I%20hope%20you%20are%20having%20a%20good%20day.
```

Die erste Zeile stellt den Endpunkt der Anforderung dar. Nach dem Endpunkt folgt ein Fragezeichen (?), das den Endpunkt von den Parametern trennt. Jeder Parameter ist durch ein kaufmännisches Und (&) vom Text getrennt.

Der Parameter `Action` gibt die auszuführende Aktion an. Eine vollständige Liste der Aktionen und die Parameter für alle Aktionen finden Sie in der [Amazon Simple Email Service API-Referenz](#) aus.

Einige Operationen verwenden Parameterlisten. Wenn Sie beispielsweise eine E-Mail an mehrere Empfänger senden, können Sie eine Liste mit E-Mail-Adressen angeben. Sie geben diese Art Liste mit der `param.n`-Notation an. Die Werte für `n` sind Ganzzahlen ab 1. Geben Sie z. B. die ersten „To:“ Verwenden Sie `Destination.ToAddresses.1`, die zweite mit `Destination.ToAddresses.2`, usw.

In Amazon SES sind Leerzeichen in Parameterwerten nicht zulässig. In diesem Handbuch werden alle Beispiele zu Anforderungsparametern mit Leerzeichen auf eine von zwei Arten angezeigt:

- URL-kodiert (als `%20`).
- Durch ein Pluszeichen („+“) dargestellt. Innerhalb einer Anforderung ist ein Pluszeichen als Kurznotation für ein Leerzeichen reserviert. (Wenn Sie ein nicht interpretiertes Pluszeichen in einen beliebigen Parameter einbeziehen möchten, müssen Sie dieses als `%2B` URL-codieren.)

Note

Jede Anfrage muss einen `x-Amzn-Authorization`-HTTP-Header haben. Weitere Informationen finden Sie unter [Authentifizieren von Anforderungen an die Amazon SES API \(p. 444\)](#).

Struktur einer POST-Anforderung

Amazon SES akzeptiert auch POST-Anfragen. Mit einer POST-Anforderung senden Sie die Parameter als Formular im HTTP-Anforderungstext, wie im folgenden Verfahren beschrieben.

So erstellen Sie eine POST-Anforderung

1. Stellen Sie die Namen und Werte der Parameter in einem Formular zusammen.

Stellen Sie die Parameter und Werte wie bei einer GET-Anforderung zusammen (mit einem kaufmännischen Und zum Trennen jedes Name-Wert-Paares). Das folgende Beispiel zeigt eine `SendEmail`-Anforderung mit den Zeilenumbrüchen, die in diesem Handbuch verwendet werden, damit die Informationen übersichtlicher sind.

```
Action=SendEmail
```

```
&Source=user@example.com
&Destination.ToAddresses.member.1=allan@example.com
&Message.Subject.Data=This is the subject line.
&Message.Body.Text.Data=Hello. I hope you are having a good day.
```

2. URL-codieren Sie das Formular entsprechend dem "Form Submission"-Abschnitt der HTML-Spezifikation.

Weitere Informationen finden Sie unter http://www.w3.org/MarkUp/html-spec/html-spec_toc.html#SEC8.2.1.

```
Action=SendEmail
&Source=user%40example.com
&Destination.ToAddresses.member.1=allan%40example.com
&Message.Subject.Data=This%20is%20the%20subject%20line.
&Message.Body.Text.Data=Hello.%20I%20hope%20you%20are%20having%20a%20good%20day.
```

3. Stellen Sie das resultierende Formular als Text der POST-Anforderung bereit.
4. Binden Sie die folgenden HTTP-Header in die Anfrage ein:
 - Content-Type mit dem Wert `application/x-www-form-urlencoded`
 - Content-Length
 - Date
 - Authorization (Weitere Informationen finden Sie unter [Authentifizieren von Anforderungen an die Amazon SES API \(p. 444\)](#).)
5. Senden Sie die vollständige Anfrage.

```
POST / HTTP/1.1
Date: Thu, 26 May 2011 06:49:50 GMT
Host: email.us-west-2.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE, SignedHeaders=Date;x-amz-date, Signature=9d63c3b5b7623d1fa3dc7fd1547313b9546c6d0fbbb6773a420613b7EXAMPLE
Content-Length: 230

Action=SendEmail
&Source=user%40example.com
&Destination.ToAddresses.member.1=allan%40example.com
&Message.Subject.Data=This%20is%20the%20subject%20line.
&Message.Body.Text.Data=Hello.%20I%20hope%20you%20are%20having%20a%20good%20day.
```

Note

Ihr HTTP-Client fügt der HTTP-Anforderung in der Regel andere Elemente entsprechend den Anforderungen der vom Client verwendeten HTTP-Version hinzu. Diese zusätzlichen Elemente sind in den Beispielen dieses Handbuchs nicht enthalten.

Authentifizieren von Anforderungen an die Amazon SES API

Wenn Sie auf die Amazon SES S-API zugreifen, authentifizieren Sie Ihre Anforderung mit der AWS - Signatur. Wenn Ihre Anforderung keine gültige Signatur enthält, gibt Amazon SES einen Fehler zurück und die Anforderung wird nicht verarbeitet.

Weitere Informationen zum Signieren von AWS Anforderungen finden Sie unter [Signieren von AWS-Anforderungen](#) im Allgemeinen AWS-Referenz.

Important

Ab dem 1. Oktober 2020 unterstützt Amazon SES nur Anforderungen, die mit Signature Version 4 signiert wurden. Wenn Sie eine ältere Version der AWS-Signatur verwenden, müssen Sie vor diesem Datum zu AWS-Signaturversion 4 wechseln.

Authentifizierungsfehler

Wenn Sie versuchen, E-Mails zu senden, und Ihre Anforderung eine frühere Version der AWS Signature verwendet, wird eine Fehlermeldung ähnlich der folgenden angezeigt:

```
<ErrorResponse xmlns="http://ses.amazonaws.com/doc/2010-12-01/">
  <Error>
    <Type>Sender</Type>
    <Code>InvalidClientTokenId</Code>
    <Message>The security token included in the request is invalid</Message>
  </Error>
</ErrorResponse>
```

Dieser Fehler kann angezeigt werden, wenn Sie eine ältere Version eines AWS SDKs oder der verwenden AWS CLI. Dieser Fehler kann auch angezeigt werden, wenn Sie eine direkte HTTPS-Anforderung an die Amazon SES S-API senden, die eine ältere Version der AWS -Signatur verwendet.

Wenn diese Fehlermeldung angezeigt wird, müssen Sie Ihre Anforderungen aktualisieren, um AWS Signature Version 4 zu verwenden, indem Sie Ihre vorhandenen SMTP-Anmeldeinformationen entsprechend der entsprechenden Vorgehensweise ersetzen:

- Wenn Sie Ihre SMTP-Anmeldeinformationen mit der SES-Konsole generiert haben, erstellen Sie einfach neue Anmeldeinformationen und ersetzen Sie Ihre vorhandenen Anmeldeinformationen durch die neuen.
- Wenn Sie Ihre SMTP-Anmeldeinformationen aus Ihren AWS Anmeldeinformationen abgeleitet haben, stellen Sie sicher, dass Sie den AWS Signature Version 4-Algorithmus verwenden. Wenn Sie sich für diese Konvertierung auf eine Bibliothek verlassen, überprüfen Sie, ob die Bibliothek über eine neuere Version verfügt, die den AWS Signature Version 4-Algorithmus verwendet, und migrieren Sie sie. Andernfalls müssen Sie entweder die Anmeldeinformationen aus einer anderen Bibliothek ableiten, die den AWS Signature Version 4-Algorithmus verwendet, oder Anmeldeinformationen mithilfe der SES-Konsole generieren.

Migration auf AWS Signature Version 4

Wenn Sie ein AWS -SDK oder die AWS CLI Wenn Sie ein Update auf die neueste Version des SDKs oder der ausführen, sollten Sie ein Update auf die AWS CLI. Wenn Sie direkte HTTPS-Anforderungen an die Amazon SES S-API senden, aktualisieren Sie die Header in Ihren Anforderungen so, dass AWS Signature Version 4 verwendet wird. Sie können API-Anforderungen, die frühere Versionen der AWS -Signatur verwenden, leicht identifizieren, indem Sie sich die Header der Anforderung ansehen. Beispielsweise ähneln Anforderungen, die AWS Signature Version 3 verwenden, dem folgenden Beispiel.

```
X-Amzn-Authorization: AWS3-HTTPS
AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE,Algorithm=HMACSHA256,Signature=lBP67vCvGl ...
```

Anforderungen, die AWS Signature Version 4 verwenden, enthalten den `Authorization` Header, der die folgenden Informationen enthält:

- Der Algorithmus, den Sie zum Signieren verwendet haben (AWS4-HMAC-SHA256)
- Der Umfang der Anmeldeinformationen (mit Ihrer Zugriffsschlüssel-ID)
- Eine Liste signierter Header
- Die berechnete Signatur. Die Signatur basiert auf den Informationen Ihrer Anforderung. Zur Erstellung der Signatur verwenden Sie den geheimen AWS-Zugriffsschlüssel. Die Signatur bestätigt AWS Ihre Identität.

Ein Beispiel für einen Aufruf der Amazon SES S-API, die AWS Signature Version 4 verwendet, finden Sie unter [Amazon SES Anforderungen](#) (p. 442). Weitere Informationen zur Verwendung der AWS Signature Version 4 finden Sie unter [Prozess mit Signatur Version 4](#) im Allgemeinen AWS-Referenz.

GET- und POST-Beispiele für die -API

Dieser Abschnitt enthält Beispiele für Anforderungen, die Sie an die -AAmazon SES können.

Beispiel für GET-Anforderung

Der folgende Code ist ein Beispiel für eine GET-Anforderung. Er enthält eine berechnete Signatur. Beachten Sie, dass alle Parameter in der Anforderung URL-kodiert sind.

```
https://email.us-west-2.amazonaws.com/  
?Action=SendEmail  
&Source=user%40example.com  
&Destination.ToAddresses.member.1=allan%40example.com  
&Message.Subject.Data=This%20is%20the%20subject%20line.  
&Message.Body.Text.Data=Hello.%20I%20hope%20you%20are%20having%20a%20good%20day.  
&AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE  
&Signature=RhU864jFu893mg7g9N9j9nr6h7EXAMPLE  
&Algorithm=HMACSHA256
```

Beispiel für POST-Anforderung

Der folgende Code ist ein Beispiel für eine POST-Anforderung. Er enthält eine berechnete Signatur. Beachten Sie, dass alle Parameter in der Anforderung URL-kodiert sind.

```
POST / HTTP/1.1  
Host: email.us-west-2.amazonaws.com  
Content-Type: application/x-www-form-urlencoded  
Date: Tue, 25 May 2010 21:20:27 +0000  
Content-Length: 174  
  
Action=SendRawEmail  
&Destinations.member.1=allan%40example.com  
&RawMessage.Data=RnJvbTp1c2VyQG9V4YW1wbGUy29tDQpTdWJqZWNO0iBUZXN0DQoNCk1lc3 ...
```

Der Wert für `RawMessage.Data` ist eine mit Base64 codierte Darstellung des folgenden Texts.

```
From:user@example.com  
Subject: Test  
  
Message sent using SendRawEmail.
```

Im Folgenden finden Sie eine vollständige POST-Anforderung an den `SendRawEmail`-Operator. Die Anforderung enthält den `X-Amzn-Authorization-Header`. Keiner der Header ist URL-kodiert.

```
POST / HTTP/1.1
Host: email.us-west-2.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Date: Tue, 25 May 2010 21:20:27 +0000
Content-Length: 174
Authorization: AWS4-HMAC-SHA256 Credential=AKIDEXAMPLE/20150830/us-east-1/iam/aws4_request,
SignedHeaders=content-type;host;x-amz-date,Signature=5d672d79c1EXAMPLE

Action=SendRawEmail
&Destinations.member.1=allan%40example.com
&RawMessage.Data=RnJvbTp1c2VyQG9V4YW1wbGUuY29tDQpTdWJqZWNoOiBUZXN0DQoNCk1lc3 ...
```

Amazon SES -API-Antworten

Amazon SES gibt als Antwort auf eine -API-Anforderung eine XML-Datenstruktur mit den Ergebnissen der Anforderung zurück.

Jede Amazon SES Antwort enthält eine Anforderungs-ID in einem `RequestId`-Element. Der Wert stellt eine eindeutige Zeichenfolge dar, die AWS zuweist. Wenn es mit einer bestimmten Anforderung Probleme gibt, fragt AWS bei der Fehlerbehebung nach der Anforderungs-ID.

Erfolgreiche Amazon SES S-Antworten enthalten außerdem eine oder mehrere Mitteilungs-IDs. Sie können sich eine Mitteilungs-ID als Beleg für eine von Amazon SES gesendete E-Mail-Nachricht vorstellen. Wenn eine Nachricht abgelehnt wurde oder unzustellbar war, ist die Mitteilungs-ID in jeder erhaltenen Benachrichtigung zu unzustellbaren E-Mails oder Beschwerden enthalten. Sie können die Mitteilungs-ID nutzen, um gesendete problematische E-Mail-Nachrichten zu identifizieren und entsprechende Maßnahmen zu ergreifen.

Struktur einer erfolgreichen Antwort

Wenn die Anforderung erfolgreich war, wird das Hauptantwortelement nach der Aktion benannt, allerdings mit dem Zusatz "Antwort". `SendEmailResponse` ist beispielsweise das Antwortelement, das für eine erfolgreiche `SendEmail`-Anforderung zurückgegeben wird. Dieses Element enthält die folgenden untergeordneten Elemente:

- `ResponseMetadata` mit dem untergeordneten Element `RequestId`.
- Ein optionales Element, das die aktionsspezifischen Ergebnisse enthält. Das `SendEmailResponse`-Element enthält beispielsweise ein Element mit dem Namen `SendEmailResult`.

Das XML-Schema beschreibt die XML-Antwortnachricht für jede Amazon SES Aktion.

Nachfolgend finden Sie ein Beispiel für eine erfolgreiche Antwort.

```
<SendEmailResponse xmlns="https://email.amazonaws.com/doc/2010-03-31/">
  <SendEmailResult>
    <MessageId>000001271b15238a-fd3ae762-2563-11df-8cd4-6d4e828a9ae8-000000</MessageId>
  </SendEmailResult>
  <ResponseMetadata>
    <RequestId>fd3ae762-2563-11df-8cd4-6d4e828a9ae8</RequestId>
  </ResponseMetadata>
</SendEmailResponse>
```

Struktur einer Amazon SES Fehlerantwort

Falls eine Anforderung nicht erfolgreich war, hat das Hauptantwortelement ungeachtet der aufgerufenen Aktion den Namen `ErrorResponse`. Dieses Element enthält ein `Error`- und ein `RequestId`-Element. Jedes `Error`-Element umfasst Folgendes:

- Ein `Type`-Element, anhand dessen identifiziert wird, ob es sich bei dem Fehler um einen Empfänger- oder einen Senderfehler handelt
- ein `Code`-Element zum Identifizieren des aufgetretenen Fehlertyps
- ein `Message`-Element, das die Fehlerbedingung in lesbarer Form beschreibt
- ein `Detail`-Element, das zusätzliche Details zu dem Fehler enthalten oder leer sein kann

Nachfolgend finden Sie ein Beispiel für eine Fehlerantwort.

```
<ErrorResponse>
  <Error>
    <Type>
      Sender
    </Type>
    <Code>
      ValidationError
    </Code>
    <Message>
      Value null at 'message.subject' failed to satisfy constraint: Member must not be
      null
    </Message>
  </Error>
  <RequestId>
    42d59b56-7407-4c4a-be0f-4c88daeea257
  </RequestId>
</ErrorResponse>
```

Von der Amazon SES API zurückgegebene Fehlercodes

Dieses Thema enthält eine Liste der von der Amazon SES API zurückgegebenen Fehlercodes. Weitere Informationen zur Amazon SES API finden Sie unter [Amazon Simple Service API-Referenz](#) aus.

Sie sollten HTTPS-Anfragen wiederholen, die 5xx-Fehler erhalten. In diesem Fall und um die Wahrscheinlichkeit einer Duplikatgenerierung zu verringern, wird empfohlen, eine exponentielle Wiederholungsmethode mit progressiv längeren Wartezeiten (5, 10 und 30 Sekunden) zwischen aufeinanderfolgenden Zeitüberschreitungen zu implementieren. Führen Sie im Fall, dass der dritte Aufrufversuch nicht erfolgreich ist, eine weitere Reihe von Wiederholungsversuchen nach 20 Minuten durch. Eine Beispielimplementierung, die eine exponentielle Wiederholungsrichtlinie mit Amazon SES verwendet, finden Sie unter [How to handle a „Throttling - Maximum sending rate exceeded“ error](#) im Amazon SES -Blog.

Note

AWS/SDKs implementieren die Logik für Wiederholversuche [automatisch](#).

HTTPS-Client-Fehler (4xx) weisen darauf hin, dass die Anforderung geändert werden muss, um das Problem zu beheben. Erst dann sollte sie wiederholt werden. Wenn beispielsweise Ihre Anmeldeinformationen für die AWS-Authentifizierung ungültig sind, müssen Sie Ihre Konfiguration

aktualisieren, damit die richtigen Anmeldeinformationen verwendet werden, bevor die E-Mail erneut gesendet wird.

Fehler	Beschreibung	HTTPS-Statuscode	Aktionen, die diesen Code zurückgeben
ConfigurationSetDoesNotExist	Die 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 mit Amazon SES Ereignisveröffentlichung (p. 313).	400	SendEmail, SendRawEmail
IncompleteSignature	The request signature does not conform to AWS standards.	400	Alle
InternalFailure	Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.	500	Alle
InvalidAction	Die angeforderte Aktion oder Operation ist ungültig. Überprüfen Sie, ob die Aktion ordnungsgemäß eingegeben wurde.	400	Alle
InvalidClientTokenId	Das angegebene X.509-Zertifikat oder die AWS-Zugriffsschlüssel-ID ist nicht in unseren Datensätzen vorhanden.	403	Alle
InvalidParameterCombination	Parameter, die nicht gemeinsam verwendet werden dürfen, wurden gemeinsam verwendet.	400	Alle
InvalidParameterValue	Für den Eingabeparameter wurde ein ungültiger Wert oder ein Wert angegeben, der sich außerhalb des gültigen Bereichs befindet.	400	Alle

Fehler	Beschreibung	HTTPS-Statuscode	Aktionen, die diesen Code zurückgeben
InvalidQueryParameter	Die AWS-Abfragezeichenfolge ist falsch formatiert und entspricht nicht den AWS-Standards.	400	Alle
MailFromDomainNotVerified	Die Nachricht konnte nicht gesendet werden, da Amazon SES den MX-Datensatz nicht lesen konnte, der für die Verwendung der angegebenen MAIL FROM-Domäne erforderlich ist.	400	SendEmail, SendRawEmail
MalformedQueryString	Die Abfragezeichenfolge enthält einen Syntaxfehler.	404	Alle
MessageRejected	Gibt an, dass die Aktion fehlgeschlagen ist und die Nachricht nicht gesendet werden konnte. Überprüfen Sie den Fehler-Stack auf eine Beschreibung dessen, was den Fehler verursacht hat. Weitere Informationen über Probleme, durch die dieser Fehler verursacht werden kann, finden Sie unter Fehler beim Senden von Amazon SES E-Mails über (p. 515) .	400	SendEmail, SendRawEmail
MissingAction	In der Anforderung fehlt ein Aktions- oder ein erforderlicher Parameter.	400	Alle
MissingAuthenticationToken	Die Anforderung muss eine gültigen (registrierte) AWS-Zugriffsschlüssel-ID oder ein X.509-Zertifikat enthalten.	403	Alle
MissingParameter	Ein erforderlicher Parameter für die festgelegte Aktion ist nicht angegeben.	400	Alle

Fehler	Beschreibung	HTTPS-Statuscode	Aktionen, die diesen Code zurückgeben
OptInRequired	Die AWS-Zugriffsschlüssel-ID benötigt ein Abonnement für den Service.	403	Alle
RequestExpired	Die Anforderung hat den Service mehr als 15 Minuten nach dem Datumsstempel oder mehr als 15 Minuten nach dem Ablaufdatum der Anforderung erreicht (z. B. für vorsignierte URLs) oder der Datumsstempel auf der Anforderung liegt mehr als 15 Minuten in der Zukunft.	400	Alle
ServiceUnavailable	Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.	503	Alle
Drosselung	Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.	400	Alle

Amazon SES Codebeispiele

In diesem Abschnitt finden Sie Codebeispiele für die ersten Schritte mit Amazon SES, damit Sie E-Mails senden und Ihr Amazon SES-Konto verwalten können. Codebeispiele sind in den folgenden Sprachen verfügbar: [C#](#), [Go](#), [Java](#), [PHP](#), [Python](#), und [Ruby](#).

Klicken Sie auf einen der folgenden Links, um das Codebeispiel für die jeweilige Aufgabe aufzurufen:

- [Senden von E-Mails mit AWS SDKs \(p. 452\)](#)
- [Senden von E-Mails über die Amazon SES SMTP-Schnittstelle \(p. 466\)](#)
- [Senden von Raw-E-Mails mit AWS SDKs \(p. 478\)](#)
- [Verifizieren mehrerer E-Mail-Adressen \(p. 487\)](#)
- [Replizieren von E-Mail-Identitäten über AWS Regionen hinweg \(p. 488\)](#)

Senden von E-Mails mit AWS SDKs

Die AWS S-SDKs enthalten integrierte Methoden für die Interaktion mit Amazon SES und mit zahlreichen anderen AWS -Services. Wenn Sie Amazon SES zusammen mit anderen AWS -Services nutzen möchten, sollten Sie ein SDK verwenden. Weitere Informationen zu den AWS -SDKs finden Sie unter [Tools für Amazon Web Services](#)

In diesem Abschnitt finden Sie Codebeispiele in verschiedenen Programmiersprachen, die das Verfahren zum Senden von E-Mails über Amazon SES mithilfe der AWS S-SDKs veranschaulichen.

C#

Das folgende Codebeispiel ist eine Komplettlösung, um mit dem E-Mails über Amazon SES mit dem [AWS SDK for .NET](#). In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for .NET installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei \(p. 34\)](#).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel im SDK Store angeben. Weitere Informationen finden Sie unter [Konfigurieren der AWS Anmeldeinformationen](#) im AWS SDK for .NET Entwicklerhandbuch. Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
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 for .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 for .NET.";

    // The HTML body of the email.
    static readonly string htmlBody = @"<html>
<head></head>
<body>
    <h1>Amazon SES Test (AWS SDK for .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 for .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();
}
}
```

Go

Das folgende Codebeispiel ist eine Komplettlösung, um mit dem E-Mails über Amazon SES mit dem [AWS SDK for Go](#). In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for Go installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie zwei Umgebungsvariablen (`AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY`, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
package main

import (
    "fmt"

    //go get -u 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/awsserr"
)

const (
    // 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 out the following constant and the
// ConfigurationSetName: aws.String(ConfigurationSet) argument below
ConfigurationSet = "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 for Go)"

// The HTML body for the email.
HtmlBody = "<h1>Amazon SES Test Email (AWS SDK for Go)</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-go/'>AWS SDK for Go</a>.</p>"

//The email body for recipients with non-HTML email clients.
TextBody = "This email was sent with Amazon SES using the AWS SDK for Go."

// The character encoding for the email.
CharSet = "UTF-8"
)

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)

    // Assemble the email.
    input := &ses.SendEmailInput{
        Destination: &ses.Destination{
            CcAddresses: []*string{
            },
            ToAddresses: []*string{
                aws.String(Recipient),
            },
        },
        Message: &ses.Message{
            Body: &ses.Body{
                Html: &ses.Content{
                    CharSet: aws.String(CharSet),
                    Data:    aws.String(HtmlBody),
                },
                Text: &ses.Content{
                    CharSet: aws.String(CharSet),
                    Data:    aws.String(TextBody),
                },
            },
            Subject: &ses.Content{
                CharSet: aws.String(CharSet),
                Data:    aws.String(Subject),
            },
        },
        Source: aws.String(Sender),
        // Comment or remove the following line if you are not using a
        // configuration set
        ConfigurationSetName: aws.String(ConfigurationSet),
    }

    // Attempt to send the email.
```

```
result, err := svc.SendEmail(input)

// Display error messages if they occur.
if err != nil {
    if aerr, ok := err.(awserr.Error); ok {
        switch aerr.Code() {
            case ses.ErrCodeMessageRejected:
                fmt.Println(ses.ErrCodeMessageRejected, aerr.Error())
            case ses.ErrCodeMailFromDomainNotVerifiedException:
                fmt.Println(ses.ErrCodeMailFromDomainNotVerifiedException,
aerr.Error())
            case ses.ErrCodeConfigurationSetDoesNotExistException:
                fmt.Println(ses.ErrCodeConfigurationSetDoesNotExistException,
aerr.Error())
            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("Email Sent!")
fmt.Println(result)
}
```

Java SDK v1

Das folgende Codebeispiel ist eine Komplettlösung, um mit dem E-Mails über Amazon SES mit dem [AWS SDK for Java](#). In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for Java installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

```
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 for Java)";

// The HTML body for the email.
static final String HTMLBODY = "<h1>Amazon SES test (AWS SDK for 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 for 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());
    }
}
```

Java SDK v2

Das folgende Codebeispiel ist eine Komplettlösung, um mit dem E-Mails über Amazon SES mit dem [AWS SDK for Java 2.x](#) und die [JavaMail PI](#). In diesem Codebeispiel wird davon ausgegangen, dass das SDK for Java 2.x installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

```
package com.example.ses;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
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 java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.nio.ByteBuffer;
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;

/**
 * To run this Java V2 code example, ensure that you have setup your development
 * environment, including your credentials.
 *
 * For information, see this documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
 */
public class SendMessage {

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

        final String USAGE = "\n" +
            "Usage:\n" +
            "    SendMessage <sender> <recipient> <subject> \n\n" +
            "Where:\n" +
            "    sender - an email address that represents the sender. \n"+
            "    recipient - an email address that represents the recipient. \n"+
            "    subject - the subject line. \n" ;

        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 email body for non-HTML email clients
        String bodyText = "Hello,\r\n" + "See the list of customers. ";

        // 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, bodyText, bodyHTML);
            client.close();
            System.out.println("Done");
        } catch (IOException | MessagingException e) {
            e.printStackTrace();
        }
    }

    public static void send(SesClient client,
        String sender,
        String recipient,
```

```
        String subject,
        String bodyText,
        String bodyHTML
        ) throws AddressException, MessagingException, IOException
    {

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

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

        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);  
        }  
    }  
}
```

JavaScript

Das folgende Codebeispiel ist eine Komplettlösung, um mit dem E-Mails über Amazon SES mit dem [AWS SDK für JavaScript in Node.js](#). In diesem Codebeispiel wird davon ausgegangen, dass das SDK für JavaScript in Node.js installiert ist. Node.js Zudem müssen Sie eine Konfigurationsdatei erstellen, die Ihre AWS Zugriffsschlüssel-ID, den geheimen Zugriffsschlüssel und Ihre bevorzugte AWS-Region enthält. Weitere Informationen zum Erstellen dieser Datei finden Sie unter [Loading Credentials in Node.js from a JSON File](#).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie zwei Umgebungsvariablen (`AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY`, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
'use strict';  
  
var aws = require('aws-sdk');  
  
// Provide the full path to your config.json file.  
aws.config.loadFromPath('./config.json');  
  
// Replace sender@example.com with your "From" address.  
// This address must be verified with Amazon SES.  
const 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.  
const 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.  
const configuration_set = "ConfigSet";  
  
// The subject line for the email.  
const subject = "Amazon SES Test (AWS SDK for JavaScript in Node.js)";  
  
// The email body for recipients with non-HTML email clients.  
const body_text = "Amazon SES Test (SDK for JavaScript in Node.js)\r\n"  
    + "This email was sent with Amazon SES using the "  
    + "AWS SDK for JavaScript in Node.js.";  
  
// The HTML body of the email.  
const body_html = `<html>  
<head></head>  
<body>  
    <h1>Amazon SES Test (SDK for JavaScript in Node.js)</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-node-js/'>  
    AWS SDK for JavaScript in Node.js</a>.</p>  
</body>  
</html>`;

// The character encoding for the email.  
const charset = "UTF-8";

// Create a new SES object.  
var ses = new aws.SES();

// Specify the parameters to pass to the API.  
var params = {  
  Source: sender,  
  Destination: {  
    ToAddresses: [  
      recipient  
    ],  
  },  
  Message: {  
    Subject: {  
      Data: subject,  
      Charset: charset  
    },  
    Body: {  
      Text: {  
        Data: body_text,  
        Charset: charset  
      },  
      Html: {  
        Data: body_html,  
        Charset: charset  
      }  
    }  
  },  
  ConfigurationSetName: configuration_set  
};

//Try to send the email.  
ses.sendEmail(params, function(err, data) {  
  // If something goes wrong, print an error message.  
  if(err) {  
    console.log(err.message);  
  } else {  
    console.log("Email sent! Message ID: ", data.MessageId);  
  }  
});
```

PHP

Das folgende Codebeispiel ist eine Komplettlösung, um mit dem E-Mails über Amazon SES mit dem [AWS SDK for PHP](#). In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for PHP installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie

zwei Umgebungsvariablen (AWS_ACCESS_KEY_ID und AWS_SECRET_ACCESS_KEY, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
<?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 for 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 for 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";
}
```

Python

Das folgende Codebeispiel ist eine Komplettlösung, um mit dem E-Mails über Amazon SES mit dem [AWS SDK for Python \(Boto\)](#). In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for Python (Boto) installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie zwei Umgebungsvariablen (`AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY`, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
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 for 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 for 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'])
```

Ruby

Das folgende Codebeispiel ist eine Komplettlösung, um mit dem E-Mails über Amazon SES mit dem [AWS SDK for Ruby](#). In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for Ruby installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen über die Installation des SDK for Ruby finden Sie unter [Installieren des AWS SDK for Ruby](#) im AWS SDK for Ruby Entwicklerhandbuch. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie zwei Umgebungsvariablen (`AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY`, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
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 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 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
```

Senden von E-Mails über die Amazon SES SMTP-Schnittstelle

Etliche Programmiersprachen enthalten Standardbibliotheken zum Senden von E-Mails über SMTP. Mit diesen Bibliotheken können Sie einfache und ausgesprochen konfigurierbare E-Mail-Programme erstellen.

In diesem Abschnitt finden Sie Codebeispiele in verschiedenen Programmiersprachen, die das Verfahren zum Senden von E-Mails über Amazon SES mithilfe der SMTP-Schnittstelle veranschaulichen. In den Codebeispielen werden – soweit möglich – die Standardbibliotheken verwendet.

C#

Das folgende Codebeispiel ist eine Komplettlösung, um E-Mails über die Amazon SES SMTP-Schnittstelle mit C# zu senden. Für die Ausführung dieses Codebeispiels benötigen Sie SMTP-Anmeldeinformationen. Weitere Informationen dazu finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#).

```
using System;  
using System.Net;  
using System.Net.Mail;  
  
namespace AmazonSESSample  
{  
    class Program  
    {  
        static void Main(string[] args)  
        {  
            // Replace sender@example.com with your "From" address.  
            // This address must be verified with Amazon SES.  
            String FROM = "sender@example.com";  
            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.  
            String TO = "recipient@amazon.com";  
        }  
    }  
}
```

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

// Replace smtp_password with your Amazon SES SMTP password.
String SMTP_PASSWORD = "smtp_password";

// (Optional) the name of a configuration set to use for this message.
// If you comment out this line, you also need to remove or comment out
// the "X-SES-CONFIGURATION-SET" header below.
String CONFIGSET = "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 AWS Region.
String HOST = "email-smtp.us-west-2.amazonaws.com";

// The port you will connect to on the Amazon SES SMTP endpoint. We
// are choosing port 587 because we will use STARTTLS to encrypt
// the connection.
int PORT = 587;

// The subject line of the email
String SUBJECT =
    "Amazon SES test (SMTP interface accessed using C#)";

// The body of the email
String BODY =
    "<h1>Amazon SES Test</h1>" +
    "<p>This email was sent through the " +
    "<a href='https://aws.amazon.com/ses'>Amazon SES</a> SMTP interface " +
    "using the .NET System.Net.Mail library.</p>";

// Create and build a new MailMessage object
MailMessage message = new MailMessage();
message.IsBodyHtml = true;
message.From = new MailAddress(FROM, FROMNAME);
message.To.Add(new MailAddress(TO));
message.Subject = SUBJECT;
message.Body = BODY;
// Comment or delete the next line if you are not using a configuration set
message.Headers.Add("X-SES-CONFIGURATION-SET", CONFIGSET);

using (var client = new System.Net.Mail.SmtpClient(HOST, PORT))
{
    // Pass SMTP credentials
    client.Credentials =
        new NetworkCredential(SMTP_USERNAME, SMTP_PASSWORD);

    // Enable SSL encryption
    client.EnableSsl = true;

    // Try to send the message. Show status in console.
    try
    {
        Console.WriteLine("Attempting to send email...");
        client.Send(message);
        Console.WriteLine("Email sent!");
    }
    catch (Exception ex)
    {
        Console.WriteLine("The email was not sent.");
        Console.WriteLine("Error message: " + ex.Message);
    }
}
}
```

```
}
```

Go

Das folgende Codebeispiel ist eine Komplettlösung, um E-Mails über die Amazon SES SMTP-Schnittstelle mit derGoProgrammiersprache. Für die Ausführung dieses Codebeispiels benötigen Sie SMTP-Anmeldeinformationen. Weitere Informationen dazu finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#). Außerdem muss das [Gomail-Paket](#) installiert sein.

```
package main

import (
    "fmt"
    "gopkg.in/gomail.v2" //go get gopkg.in/gomail.v2
)

const (
    // 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 SmtplibUser with your Amazon SES SMTP user name.
    SmtplibUser = "SmtplibUser"

    // Replace SmtplibPass with your Amazon SES SMTP password.
    SmtplibPass = "SmtplibPass"

    // 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.
    ConfigSet = "ConfigSet"

    // If you're using Amazon SES in an AWS 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 for the email.
    Subject = "Amazon SES Test (Gomail)"

    // The HTML body for the email.
    HtmlBody = "<html><head><title>SES Sample Email</title></head><body>" +
        "<h1>Amazon SES Test Email (Gomail)</h1>" +
        "<p>This email was sent with " +
        "<a href='https://aws.amazon.com/ses/'>Amazon SES</a> using " +
        "the <a href='https://github.com/go-gomail/gomail/'>Gomail " +
        "package</a> for <a href='https://golang.org/'>Go</a>.</p>" +
        "</body></html>"

    //The email body for recipients with non-HTML email clients.
    TextBody = "This email was sent with Amazon SES using the Gomail package."

    // The tags to apply to this message. Separate multiple key-value pairs
    // with commas.
    // If you comment out or remove this variable, you will also need to
    // comment out or remove the header on line 80.
    Tags = "genre=test,genre2=test2"
```

```
// The character encoding for the email.
Charset = "UTF-8"

)

func main() {

    // Create a new message.
    m := gomail.NewMessage()

    // Set the main email part to use HTML.
    m.SetBody("text/html", HtmlBody)

    // Set the alternative part to plain text.
    m.AddAlternative("text/plain", TextBody)

    // Construct the message headers, including a Configuration Set and a Tag.
    m.SetHeaders(map[string][]string{
        "From": {m.FormatAddress(Sender, SenderName)},
        "To": {Recipient},
        "Subject": {Subject},
        // Comment or remove the next line if you are not using a configuration set
        "X-SES-CONFIGURATION-SET": {ConfigSet},
        // Comment or remove the next line if you are not using custom tags
        "X-SES-MESSAGE-TAGS": {Tags},
    })

    // Send the email.
    d := gomail.NewPlainDialer(Host, Port, SmtplibUser, SmtplibPass)

    // Display an error message if something goes wrong; otherwise,
    // display a message confirming that the message was sent.
    if err := d.DialAndSend(m); err != nil {
        fmt.Println(err)
    } else {
        fmt.Println("Email sent!")
    }
}
```

Java

Das folgende Codebeispiel ist eine Komplettlösung, um E-Mails über die Amazon SES SMTP-Schnittstelle mit Java zu senden. Für die Ausführung dieses Codebeispiels benötigen Sie SMTP-Anmeldeinformationen. Weitere Informationen dazu finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen](#) (p. 95). Außerdem müssen Sie die [JavaMail-API](#) herunterladen.

```
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";

// Replace smtp_password with your Amazon SES SMTP password.
static final String SMTP_PASSWORD = "smtp_password";

// 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();

    // 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();
    }
}
```

JavaScript

Das folgende Codebeispiel ist eine Komplettlösung, um E-Mails über die Amazon SES SMTP-Schnittstelle mit dem [NodeMailer](#) Modul in Node.js.

Um dieses Codebeispiel ausführen zu können, müssen Sie zuerst SMTP-Anmeldeinformationen abrufen. Weitere Informationen finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#). Darüber hinaus müssen Sie das [NodeMailer](#)-Modul installieren.

```
/*
This code uses callbacks to handle asynchronous function responses.
It currently demonstrates using an async-await pattern.
AWS supports both the async-await and promises patterns.
For more information, see the following:
https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Statements/async_function
https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide/Using_promises
https://docs.aws.amazon.com/sdk-for-javascript/v2/developer-guide/calling-services-asynchronously.html
https://docs.aws.amazon.com/lambda/latest/dg/nodejs-prog-model-handler.html
*/

"use strict";
const nodemailer = require("nodemailer");

// 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 AWS Region.
const smtpEndpoint = "email-smtp.us-west-2.amazonaws.com";

// The port to use when connecting to the SMTP server.
const port = 587;

// Replace sender@example.com with your "From" address.
// This address must be verified with Amazon SES.
const senderAddress = "Mary Major <sender@example.com>";

// Replace recipient@example.com with a "To" address. If your account
// is still in the sandbox, this address must be verified. To specify
// multiple addresses, separate each address with a comma.
var toAddresses = "recipient@example.com";

// CC and BCC addresses. If your account is in the sandbox, these
// addresses have to be verified. To specify multiple addresses, separate
// each address with a comma.
var ccAddresses = "cc-recipient0@example.com,cc-recipient1@example.com";
```

```
var bccAddresses = "bcc-recipient@example.com";

// Replace smtp_username with your Amazon SES SMTP user name.
const smtpUsername = "AKIAIOSFODNN7EXAMPLE";

// Replace smtp_password with your Amazon SES SMTP password.
const smtpPassword = "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY";

// (Optional) the name of a configuration set to use for this message.
var configurationSet = "ConfigSet";

// The subject line of the email
var subject = "Amazon SES test (Nodemailer)";

// The email body for recipients with non-HTML email clients.
var body_text = `Amazon SES Test (Nodemailer)
-----
This email was sent through the Amazon SES SMTP interface using Nodemailer.
`;

// The body of the email for recipients whose email clients support HTML content.
var body_html = `
<head></head>
<body>
  <h1>Amazon SES Test (Nodemailer)</h1>
  <p>This email was sent with <a href='https://aws.amazon.com/ses/'>Amazon SES</a>
    using <a href='https://nodemailer.com'>Nodemailer</a> for Node.js.</p>
</body>
</html>`;

// The message tags that you want to apply to the email.
var tag0 = "key0=value0";
var tag1 = "key1=value1";

async function main(){

  // Create the SMTP transport.
  let transporter = nodemailer.createTransport({
    host: smtpEndpoint,
    port: port,
    secure: false, // true for 465, false for other ports
    auth: {
      user: smtpUsername,
      pass: smtpPassword
    }
  });

  // Specify the fields in the email.
  let mailOptions = {
    from: senderAddress,
    to: toAddresses,
    subject: subject,
    cc: ccAddresses,
    bcc: bccAddresses,
    text: body_text,
    html: body_html,
    // Custom headers for configuration set and message tags.
    headers: {
      'X-SES-CONFIGURATION-SET': configurationSet,
      'X-SES-MESSAGE-TAGS': tag0,
      'X-SES-MESSAGE-TAGS': tag1
    }
  };

  // Send the email.
  let info = await transporter.sendMail(mailOptions)
```



```
    console.log("Message sent! Message ID: ", info.messageId);
  }

  main().catch(console.error);
```

Perl

Das folgende Codebeispiel ist eine Komplettlösung, um E-Mails über die Amazon SES SMTP-Schnittstelle mit Perl zu senden. Für die Ausführung dieses Codebeispiels benötigen Sie SMTP-Anmeldeinformationen. Weitere Informationen dazu finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#). Außerdem müssen die Module [Email::Sender](#), [Email::MIME](#) und [Try::Tiny](#) von [CPAN](#) installiert sein.

```
#!/usr/bin/perl
use warnings;
use strict;
use Email::Sender::Simple qw(sendmail);
use Email::Sender::Transport::SMTP;
use Email::MIME;
use Try::Tiny;

# Replace sender@example.com with your "From" address.
# This address must be verified.
my $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.
my $recipient = 'recipient@example.com';

# Replace smtp_username with your Amazon SES SMTP user name.
my $smtp_username = "smtp_username";

# Replace smtp_password with your Amazon SES SMTP password.
my $smtp_password = "smtp_password";

# (Optional) the name of a configuration set to use for this message.
# If you comment out this line, you also need to remove or comment out
# the "X-SES-CONFIGURATION-SET:" header below.
my $configset = "ConfigSet";

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

# The subject line of the email.
my $subject = "Amazon SES Test (Perl)";

# The HTML body for the email.
my $htmlbody = <<'END_HTML';
<html>
  <head></head>
  <body>
    <h1>Amazon SES SMTP Email Test</h1>
    <p>This email was sent with Amazon SES using the
      <a href='https://www.perl.org/'>Perl</a>
      <a href='http://search.cpan.org/~rjbs/Email-Sender-1.300031/'>
        Email::Sender</a> library.</p>
  </body>
</html>
END_HTML
```

```
# The email body for recipients with non-HTML email clients.
my $textbody = "Amazon SES Test\r\n"
    . "This message was sent with Amazon SES using the Perl "
    . "Email::Sender module.";

# Create the SMTP transport.
my $transport = Email::Sender::Transport::SMTP->new(
    host      => "$host",
    port      => "$port",
    ssl       => 'starttls',
    sasl_username => "$smtp_username",
    sasl_password => "$smtp_password",
);

# Build a multipart MIME message with an HTML part and a text part.
my $message = Email::MIME->create(
    attributes => {
        content_type => 'multipart/alternative',
        charset      => 'UTF-8',
    },
    header_str => [
        From      => "$sender",
        To        => "$recipient",
        Subject    => "$subject",
    ],
    parts => [
        Email::MIME->create(
            attributes => { content_type => 'text/plain' },
            body       => "$textbody",
        ),
        Email::MIME->create(
            attributes => { content_type => 'text/html' },
            body       => "$htmlbody",
        )
    ],
);

# Add the configuration set header to the MIME message.
$message->header_str_set( 'X-SES-CONFIGURATION-SET' => "$configset" );

# Try to send the email using the sendmail function from
# Email::Sender::Simple.
try {
    sendmail($message, { transport => $transport });
} catch {
    die "Error sending email: $_";
};
```

PHP

Das folgende Codebeispiel ist eine Komplettlösung, um E-Mails über die Amazon SES SMTP-Schnittstelle mit PHP zu senden. Für die Ausführung dieses Codebeispiels benötigen Sie SMTP-Anmeldeinformationen. Weitere Informationen dazu finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#). Zudem müssen Sie das [PHPMailer-Paket](#) mit [Composer](#) installieren.

```
<?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';

// Replace smtp_password with your Amazon SES SMTP password.
$passwordSmtp = 'smtp_password';

// 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 = $passwordSmtp;
    $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.
}

?>
```

Python

Das folgende Codebeispiel ist eine Komplettlösung, um E-Mails über die Amazon SES SMTP-Schnittstelle mit Python zu senden. Für die Ausführung dieses Codebeispiels benötigen Sie SMTP-Anmeldeinformationen. Weitere Informationen dazu finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen](#) (p. 95).

```
import smtplib
import email.utils
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText

# Replace sender@example.com with your "From" address.
# This address must be verified.
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.
USERNAME_SMTP = "smtp_username"

# Replace smtp_password with your Amazon SES SMTP password.
PASSWORD_SMTP = "smtp_password"

# (Optional) the name of a configuration set to use for this message.
# If you comment out this line, you also need to remove or comment out
# the "X-SES-CONFIGURATION-SET:" header below.
CONFIGURATION_SET = "ConfigSet"

# If you're using Amazon SES in an AWS 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 (Python smtplib)'

# The email body for recipients with non-HTML email clients.
BODY_TEXT = ("Amazon SES Test\r\n"
             "This email was sent through the Amazon SES SMTP "
             "Interface using the Python smtplib package."
            )

# The HTML body of the email.
BODY_HTML = ""<html>
<head></head>
<body>
```

```
<h1>Amazon SES SMTP Email Test</h1>
<p>This email was sent with Amazon SES using the
  <a href='https://www.python.org/'>Python</a>
  <a href='https://docs.python.org/3/library/smtplib.html'>
    smtplib</a> library.</p>
</body>
</html>

"""

# Create message container - the correct MIME type is multipart/alternative.
msg = MIMEMultipart('alternative')
msg['Subject'] = SUBJECT
msg['From'] = email.utils.formataddr((SENDERNAME, SENDER))
msg['To'] = RECIPIENT
# Comment or delete the next line if you are not using a configuration set
msg.add_header('X-SES-CONFIGURATION-SET', CONFIGURATION_SET)

# Record the MIME types of both parts - text/plain and text/html.
part1 = MIMEText(BODY_TEXT, 'plain')
part2 = MIMEText(BODY_HTML, 'html')

# Attach parts into message container.
# According to RFC 2046, the last part of a multipart message, in this case
# the HTML message, is best and preferred.
msg.attach(part1)
msg.attach(part2)

# Try to send the message.
try:
    server = smtplib.SMTP(HOST, PORT)
    server.ehlo()
    server.starttls()
    #smtp lib docs recommend calling ehlo() before & after starttls()
    server.ehlo()
    server.login(USERNAME_SMTP, PASSWORD_SMTP)
    server.sendmail(SENDER, RECIPIENT, msg.as_string())
    server.close()
# Display an error message if something goes wrong.
except Exception as e:
    print ("Error: ", e)
else:
    print ("Email sent!")
```

Ruby

Das folgende Codebeispiel ist eine Komplettlösung, um E-Mails über die Amazon SES SMTP-Schnittstelle mit Ruby zu senden. Für die Ausführung dieses Codebeispiels benötigen Sie SMTP-Anmeldeinformationen. Weitere Informationen dazu finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#).

```
require 'net/smtp'

# 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.
smtp_username = "smtp_username"
```

```
# Replace smtp_password with your Amazon SES SMTP password.
smtp_password = "smtp_password"

# (Optional) the name of a configuration set to use for this message.
# If you comment out this line, you also need to remove or comment out
# the "X-SES-CONFIGURATION-SET" header below.
configSet = "ConfigSet"

# If you're using Amazon SES in an AWS Region other than US West (Oregon),
# replace email-smtp.us-west-2.amazonaws.com with the Amazon SES SMTP
# endpoint in the appropriate region.
server = "email-smtp.us-west-2.amazonaws.com"
port = 587

# The subject line of the email.
subject = "Amazon SES Test (Ruby Net::SMTP library)"

# Specify the headers and body of the message as a variable.
message = [
  #Remove the next line if you are not using a configuration set
  "X-SES-CONFIGURATION-SET: #{configSet}",
  "Content-Type: text/html; charset=UTF-8",
  "Content-Transfer-Encoding: 7bit",
  "From: #{senderName} <#{sender}>",
  "To: #{recipient}",
  "Subject: #{subject}",
  "",
  "<h1>Amazon SES Test (Ruby Net::SMTP library)</h1>",
  "<p>This email was sent with \
<a href='https://aws.amazon.com/ses/'>\
Amazon SES</a> using the Ruby Net::SMTP library.</p>"
].join("\n")

# Create a new SMTP object called "smtp."
smtp = Net::SMTP.new(server, port)

# Tell the smtp object to connect using TLS.
smtp.enable_starttls

# Open an SMTP session and log in to the server using SMTP authentication.
smtp.start(server, smtp_username, smtp_password, :login)

# Try to send the message.
begin
  smtp.send_message(message, sender, recipient)
  puts "Email sent!"
# Print an error message if something goes wrong.
rescue => e
  puts e
end
```

Senden von Raw-E-Mails mit AWS SDKs

Die AWS S-SDKs enthalten integrierte Methoden für die Interaktion mit Amazon SES und mit zahlreichen anderen AWS -Services. Wenn Sie Amazon SES zusammen mit anderen AWS -Services nutzen möchten, sollten Sie ein SDK verwenden. Weitere Informationen zu den AWS -SDKs finden Sie unter [Tools für Amazon Web Services](#)

In diesem Abschnitt finden Sie Codebeispiele in verschiedenen Programmiersprachen, die das Verfahren zum Senden von Raw-E-Mails über Amazon SES mithilfe der AWS SDKs veranschaulichen.

Java

Das folgende Codebeispiel zeigt, wie die [JavaMail](#)-Library und [AWS SDK for Java](#) zum Erstellen und Senden einer Raw-E-Mail genutzt werden, die aus einem HTML-Abschnitt, einem Textabschnitt und einem Anhang besteht.

In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for Java installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie zwei Umgebungsvariablen (`AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY`, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
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 for 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!");
} catch (Exception ex) {
    System.out.println("Email Failed");
    System.err.println("Error message: " + ex.getMessage());
    ex.printStackTrace();
}
}
```

PHP

Das folgende Codebeispiel zeigt, wie das [PHPMailer](#)-Paket und das [AWS SDK for PHP](#) zum Erstellen und Senden einer Raw-E-Mail genutzt werden, die aus einem HTML-Abschnitt, einem Textabschnitt und einem Anhang besteht.

In diesem Codebeispiel wird davon ausgegangen, dass das [PHPMailer](#)-Paket mithilfe von [Composer](#) installiert wurde. Zudem wird davon ausgegangen, dass das AWS SDK for PHP installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur

Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie zwei Umgebungsvariablen (AWS_ACCESS_KEY_ID und AWS_SECRET_ACCESS_KEY, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
<?php
require 'vendor/autoload.php';
use PHPMailer\PHPMailer\PHPMailer;
use Aws\Ses\SesClient;
use Aws\Ses\Exception\SesException;

// 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';

// Specify a configuration set.
$configset = 'ConfigSet';

// Replace us-west-2 with the AWS Region you're using for Amazon SES.
$region = 'us-west-2';

$subject = 'List of customers to contact';

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

$textbody = <<<EOD
Hello,
Please see the attached file for a list of customers to contact.
EOD;

// The full path to the file that will be attached to the email.
$att = 'path/to/customers-to-contact.xlsx';

// Create an SesClient.
$client = SesClient::factory(array(
    'version' => 'latest',
    'region' => $region
));

// Create a new PHPMailer object.
$mail = new PHPMailer;

// Add components to the email.
$mail->setFrom($sender, $sendername);
$mail->addAddress($recipient);
$mail->Subject = $subject;
$mail->Body = $htmlbody;
$mail->AltBody = $textbody;
$mail->addAttachment($att);
$mail->addCustomHeader('X-SES-CONFIGURATION-SET', $configset);
```

```
// Attempt to assemble the above components into a MIME message.
if (!$mail->preSend()) {
    echo $mail->ErrorInfo;
} else {
    // Create a new variable that contains the MIME message.
    $message = $mail->getSentMIMEMessage();
}

// Try to send the message.
try {
    $result = $client->sendRawEmail([
        'RawMessage' => [
            'Data' => $message
        ]
    ]);
    // If the message was sent, show the message ID.
    $messageId = $result->get('MessageId');
    echo("Email sent! Message ID: $messageId"."\\n");
} catch (SesException $error) {
    // If the message was not sent, show a message explaining what went wrong.
    echo("The email was not sent. Error message: "
        . $error->getAwsErrorMessage()."\\n");
}

?>
```

Python

Das folgende Codebeispiel zeigt, wie das Python-[E-Mail](#)-Paket und das [AWS SDK for Python \(Boto\)](#) zum Erstellen und Senden einer Raw-E-Mail genutzt werden, die aus einem HTML-Abschnitt, einem Textabschnitt und einem Anhang besteht.

In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for Python (Boto) installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie zwei Umgebungsvariablen (`AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY`, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
import os
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

# 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 = "Customer service contact info"

# The full path to the file that will be attached to the email.
ATTACHMENT = "path/to/customers-to-contact.xlsx"

# The email body for recipients with non-HTML email clients.
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></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"

# Create a new SES resource and specify a region.
client = boto3.client('ses',region_name=AWS_REGION)

# Create a multipart/mixed parent container.
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)
```

```
# Add the attachment to the parent container.
msg.attach(att)
#print(msg)
try:
    #Provide the contents of the email.
    response = client.send_raw_email(
        Source=SENDER,
        Destinations=[
            RECIPIENT
        ],
        RawMessage={
            'Data':msg.as_string(),
        },
        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'])
```

Ruby

Das folgende Codebeispiel zeigt, wie das Ruby-MIME-Gem und das [AWS SDK for Ruby](#) zum Erstellen und Senden einer Raw-E-Mail genutzt werden, die aus einem HTML-Abschnitt, einem Textabschnitt und einem Anhang besteht.

In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for Ruby und das MIME-Gem installiert sind und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

Important

Sie verwenden eine Datei mit gemeinsam genutzten Anmeldeinformationen, um Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel übergeben. Alternativ zur Verwendung einer Datei mit gemeinsam genutzten Anmeldeinformationen können Sie Ihre AWS Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel angeben, indem Sie zwei Umgebungsvariablen (`AWS_ACCESS_KEY_ID` und `AWS_SECRET_ACCESS_KEY`, bzw.). Dieses Beispiel funktioniert nur, wenn Sie Ihre Anmeldeinformationen mit einer der folgenden Methoden angeben.

```
require 'base64' #standard library
require 'aws-sdk' #gem install aws-sdk
require 'mime' #gem install mime

# 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"

# Specify a configuration set.
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 = "Customer service contact info"

# The full path to the file that will be attached to the email.
attachment = "path/to/customers-to-contact.xlsx"

# The email body for recipients with non-HTML email clients.
textbody = ""
Hello,
Please see the attached file for a list of customers to contact.
""

# The HTML body of the email.
htmlbody = ""
<html>
<head></head>
<body>
<h1>Hello!</h1>
<p>Please see the attached file for a list of customers to contact.</p>
</body>
</html>
""

# Create a new MIME text object that contains the base64-encoded content of the
# file that will be attached to the message.
file = MIME::Application.new(Base64::encode64(open(attachment,"rb").read))

# Specify that the file is a base64-encoded attachment to ensure that the
# receiving client handles it correctly.
file.transfer_encoding = 'base64'
file.disposition = 'attachment'

# Create a MIME Multipart Mixed object. This object will contain the body of the
# email and the attachment.
msg_mixed = MIME::Multipart::Mixed.new

# Create a MIME Multipart Alternative object. This object will contain both the
# HTML and plain text versions of the email.
msg_body = MIME::Multipart::Alternative.new

# Add the plain text and HTML content to the Multipart Alternative part.
msg_body.add(MIME::Text.new(textbody, 'plain'))
msg_body.add(MIME::Text.new(htmlbody, 'html'))

# Add the Multipart Alternative part to the Multipart Mixed part.
msg_mixed.add(msg_body)

# Add the attachment to the Multipart Mixed part.
msg_mixed.attach(file, 'filename' => attachment)

# Create a new Mail object that contains the entire Multipart Mixed object.
# This object also contains the message headers.
msg = MIME::Mail.new(msg_mixed)
msg.to = { recipient => nil }
msg.from = { sender => sendername }
msg.subject = subject
msg.headers.set('X-SES-CONFIGURATION-SET', configsetname)

# 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_raw_email({
    raw_message: {
```

```
        data: msg.to_s
      }
    })
    # If the message was sent, show the message ID.
    puts "Email sent! Message ID: " + resp[0].to_s

    # If the message was not sent, show a message explaining what went wrong.
    rescue Aws::SES::Errors::ServiceError => error
      puts "Email not sent. Error message: #{error}"
    end
  end
end
```

Verifizieren mehrerer E-Mail-Adressen

Wenn Sie von einer anderen E-Mail-Lösung zu Amazon SES migrieren, verfügen Sie wahrscheinlich bereits über eine lange Liste von E-Mail-Adressen, die Sie zum Versenden von E-Mails verwenden möchten. Das Python-Skript in diesem Beispiel akzeptiert eine JSON-formatierte Liste von E-Mail-Adressen als Eingabe. Das folgende Beispiel zeigt die Struktur der Eingabedatei:

```
[
  {
    "email": "carlos.salazar@example.com"
  },
  {
    "email": "mary.major@example.co.uk"
  },
  {
    "email": "wei.zhang@example.cn"
  }
]
```

Das folgende Skript liest die Eingabedatei und versucht, alle in der Datei enthaltenen E-Mail-Adressen zu validieren. In diesem Codebeispiel wird davon ausgegangen, dass das AWS SDK for Python (Boto) installiert ist und eine Datei mit gemeinsam genutzten Anmeldeinformationen erstellt wurde. Weitere Informationen zum Erstellen einer Datei mit gemeinsam genutzten Anmeldeinformationen finden Sie unter [Erstellen einer freigegebenen Anmeldeinformationsdatei](#) (p. 34).

```
import json      #Python standard library
import boto3     #sudo pip install boto3
from botocore.exceptions import ClientError

# The full path to the file that contains the identities to be verified.
# The input file must be JSON-formatted. See
# https://docs.aws.amazon.com/ses/latest/DeveloperGuide/sample-code-bulk-verify.html
# for a sample input file.
FILE_INPUT = '/path/to/identities.json'

# If necessary, replace us-west-2 with the AWS Region you're using for Amazon SES.
AWS_REGION = "us-west-2"

# Create a new SES resource specify a region.
client = boto3.client('ses', region_name=AWS_REGION)

# Read the file that contains the identities to be verified.
with open(FILE_INPUT) as data_file:
    data = json.load(data_file)

# Iterate through the array from the input file. Each time an object named
# 'email' is found, run the verify_email_identity operation against the value
# of that object.
```

```
for i in data:
    try:
        response = client.verify_email_identity(
            EmailAddress=i['email']
        )
        # Display an error if something goes wrong.
    except ClientError as e:
        print(e.response['Error']['Message'])
    # Otherwise, show the request ID of the verification message.
    else:
        print('Verification email sent to ' + i['email'] + '. Request ID: ' +
              response['ResponseMetadata']['RequestId'])
```

Replizieren von E-Mail-Identitäten über AWS Regionen hinweg

Wenn Sie dieselbe Identität zum Versenden von E-Mails in mehr als einer AWS Region verwenden möchten, müssen Sie diese Identität in jeder Region verifizieren. Das Python-Skript in diesem Beispiel vereinfacht die Überprüfung einer Identität in einer neuen Region, wenn Sie sie bereits in einer anderen Region verifiziert haben.

Sie können dieses Skript verwenden, um entweder E-Mail-Adresse oder Domänenidentitäten zu replizieren. Wenn Sie dieses Skript verwenden, um eine E-Mail-Adresse zu replizieren, müssen Sie auf den Bestätigungslink in der E-Mail klicken, die Amazon SES an diese Adresse sendet. Sie können dieses Skript nur verwenden, um eine Domänenidentität zu replizieren, wenn die DNS-Einstellungen für diese Domäne von Route 53 verwaltet werden.

Note

Ihre -Sandbox- und Kontokontingente sind für jede AWS Region eindeutig. Mit anderen Worten: Wenn Ihr Konto aus der Amazon SES Sandbox in einer Region entfernt wurde, müssen Sie es dennoch in jeder anderen Region entfernen. Weitere Informationen darüber, wie Ihr Konto aus der Amazon SES -Sandbox entfernt werden kann, finden Sie unter [Verlassen der Amazon SES -Sandbox \(p. 79\)](#). Weitere Informationen zum Erhöhen Ihrer Amazon SES Servicekontingente finden Sie unter [Erhöhen Ihrer Amazon SES Versandkontingente \(p. 159\)](#).

```
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()

```

Regionen und Amazon SES

Amazon SES ist in mehreren AWS Regionen auf der ganzen Welt verfügbar. In jeder Region unterhält AWS 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 Amazon SES Regional-Endpunkte finden Sie unter [Amazon Simple Email Service-Endpunkte und Kontingente](#) im Allgemeinen Amazon Web Services Referenz. Weitere Informationen über die in jeder Region verfügbare Anzahl von Availability Zones finden Sie unter [Globale AWS-Infrastruktur](#).

Dieser Abschnitt enthält Informationen zur geplanten Verwendung von Amazon SES in mehreren AWS Regionen. Es werden die folgenden Themen behandelt:

- [Amazon SES Regionen und -Endpunkte](#) (p. 494)
- [Erhöhte Sandbox- und Sendelimits](#) (p. 495)
- [Verifizierung von E-Mail-Adressen und Domains](#) (p. 495)
- [Easy DKIM](#) (p. 495)
- [Unterdrückungsliste](#) (p. 495)
- [Feedback-Benachrichtigungen](#) (p. 495)
- [SMTP-Anmeldeinformationen](#) (p. 496)
- [Sendeautorisierung](#) (p. 497)
- [Benutzerdefinierte MAIL FRO](#) (p. 496)
- [Empfangen von E-Mails](#) (p. 497)

Allgemeine Informationen zu AWS Regionen finden Sie unter [AWS-Regionen und -Endpunkte](#) im Allgemeinen AWS Referenz.

Amazon SES Regionen und -Endpunkte

Wenn Sie Amazon Simple Email Service (Amazon SES) zum Senden von E-Mails verwenden, stellen Sie eine Verbindung zu einer URL her, die einen Endpunkt für die Amazon SES API- oder SMTP-Schnittstelle bereitstellt. Die Allgemeine AWS-Referenz enthält eine vollständige Liste der Endpunkte, die Sie zum Senden und Empfangen von E-Mails über Amazon SES verwenden. Weitere Informationen finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) im Allgemeinen AWS-Referenz.

Wenn Sie E-Mails über Amazon SES senden, können Sie die -URLs im API-(HTTPS)-Endpunkt, um HTTPS-Anfragen an die Amazon SES API zu senden. Sie können auch die URLs in der Spalte SMTP-Endpunkt verwenden, um E-Mails über die SMTP-Schnittstelle zu versenden.

Wenn Sie Amazon SES für den Empfang von E-Mails konfiguriert haben, die an Ihre Domäne gesendet werden, können Sie die eingehenden SMTP-Endpunkt-URLs (d. h. die mit „inbound-smtp“ beginnenden URLs) verwenden, wenn Sie [Einrichten der Mail Exchanger \(MX\) -Datensätze in den DNS-Einstellungen für Ihre Domäne](#) (p. 233).

Note

Die eingehenden SMTP-URLs sind keine IMAP-Server-Adressen. Mit anderen Worten: Sie können auf diese Weise keine E-Mails über eine Anwendung wie Outlook empfangen. Informationen zu einem Service mit einem IMAP-Server für eingehende E-Mails finden Sie unter [Amazon WorkMail](#).

Erhöhte Sandbox- und Sendelimits

Der Sandbox-Status für Ihr Konto kann zwischen AWS Regionen unterschiedlich sein. Mit anderen Worten: Wenn Ihr Konto aus der Sandbox in der Region USA West (Oregon) entfernt wurde, kann es sich in der Sandbox in der Region USA Ost (Nord-Virginia) weiterhin in der Sandbox befinden, außer es wurde auch aus der Sandbox in dieser Region entfernt.

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

Wenn Sie [Senden Sie eine Anfrage zur Entfernung Ihres Kontos aus der Sandbox \(p. 79\)](#), oder wenn Sie [eine Anfrage zur Erhöhung der Sendekontingente Ihres Kontos einreichen \(p. 159\)](#) Wählen Sie alle AWS Regionen aus, für die Ihre Anfrage gilt. Sie können in einem einzelnen Support-Center-Fall mehrere Anfragen senden.

Verifizierung von E-Mail-Adressen und Domains

Bevor Sie E-Mails mit Amazon SES senden können, müssen Sie sicherstellen, dass Sie Eigentümer der E-Mail-Adresse oder Domänen sind, von der Sie senden möchten. Der Verifizierungsstatus von E-Mail-Adressen und Domänen unterscheidet sich zwischen AWS Regionen. Wenn Sie z. B. eine Domäne in der Region USA West (Oregon) verifizieren, können Sie diese Domäne nicht zum Senden von E-Mails in der Region USA Ost (Nord-Virginia) verwenden, bis Sie den Verifizierungsprozess für diese Region erneut abgeschlossen haben. Weitere Informationen zur Verifizierung von E-Mail-Adressen und Domänen finden Sie unter [Überprüfen von Identitäten in Amazon SES \(p. 52\)](#).

Easy DKIM

Sie müssen den Easy DKIM-Einrichtungsprozess für jede Region durchführen, in der Sie Easy DKIM verwenden möchten. Das bedeutet, dass Sie TXT-Datensätze in jeder Region über die Amazon SES -Konsole oder die Amazon SES API generieren müssen. Anschließend müssen Sie alle TXT-Datensätze der DNS-Konfiguration für Ihre Domäne hinzufügen. Weitere Informationen zum Einrichten von Easy DKIM finden Sie unter [Einfache DKIM in Amazon SES \(p. 143\)](#).

Unterdrückungsliste

Obwohl jede Region über eine separate globale Unterdrückungsliste verfügt, entfernt Amazon SES die Adresse aus der globalen Unterdrückungsliste in allen Regionen, wenn Sie eine Adresse aus der globalen Unterdrückungsliste aus der globalen Unterdrückungsliste in allen Regionen entfernen. Sie entfernen Adressen aus der Unterdrückungsliste, indem Sie die Amazon SES -Konsole verwenden. Weitere Informationen zum Entfernen von Adressen aus der Unterdrückungsliste finden Sie unter [Verwenden der globalen Unterdrückungsliste von Amazon SES \(p. 210\)](#).

Feedback-Benachrichtigungen

Es gibt zwei wichtige Punkte, die bei der Einrichtung von Feedback-Benachrichtigungen in mehreren Regionen zu beachten sind:

- Verifizierte Identitätseinstellungen, wie z.B. ob Sie Feedback per E-Mail oder über Amazon Simple Notification Service (Amazon SNS) erhalten, gelten nur für die Region, in der Sie sie eingestellt haben.

Wenn Sie z. B. `user@example.com` in den Regionen USA West (Oregon) und USA Ost (Nord-Virginia) verwenden und nicht zugestellte E-Mails über Amazon SNS Benachrichtigungen erhalten möchten, müssen Sie die Amazon SES API oder die Amazon SES -Konsole verwenden, um Amazon SNS-Feedback-Benachrichtigungen für `user@example.com` in beiden Regionen.

- Amazon SNS Themen, die Sie für die Feedback-Weiterleitung verwenden, müssen sich in derselben Region befinden, in der Sie Amazon SES verwenden.

SMTP-Anmeldeinformationen

Die Anmeldeinformationen, die Sie zum Senden von E-Mails über die Amazon SES SMTP-Schnittstelle verwenden, sind für jede AWS Region eindeutig. Wenn Sie Amazon SES SMTP-Schnittstelle zum Senden von E-Mails in mehreren -Regionen verwenden, müssen Sie [Generieren eines Satzes von SMTP-Anmeldeinformationen \(p. 95\)](#) für jede -Region.

Note

Wenn Sie Ihre SMTP-Anmeldeinformationen vor dem 10. Januar 2019 erstellt haben, wurden Ihre SMTP-Anmeldeinformationen mit einer älteren Version der AWS Signatur erstellt. Aus Sicherheitsgründen sollten Sie Anmeldeinformationen löschen, die Sie vor diesem Datum erstellt haben, und durch neuere Anmeldeinformationen ersetzen. Sie haben folgende Möglichkeiten [Sie löschen Sie ältere Anmeldeinformationen mit der IAM-Konsole](#).

Benutzerdefinierte MAIL FROM

Sie können dieselbe benutzerdefinierte MAIL FROM-Domäne für verifizierte Identitäten in verschiedenen AWS Regionen verwenden. Wenn Sie das möchten, müssen Sie nur einen MX-Eintrag auf dem DNS-Server der „MAIL FROM“-Domäne veröffentlichen. In diesem Fall werden unzustellbare Benachrichtigungen an den Amazon SES -Feedback-Endpunkt in der Region gesendet, die Sie im MX-Eintrag angegeben haben. Als Nächstes Amazon SES leitet die Unzustellbarkeit an die verifizierte Identität in der Region um, in der die E-Mail gesendet wurde.

Verwenden Sie die Einstellungen für den MX-Eintrag, die Amazon SES während der benutzerdefinierten MAIL FROM-Einrichtung für eine Identität in einer der Regionen bereitstellt. Der benutzerdefinierte MAIL FROM Einrichtungsvorgang ist in [Einrichten einer benutzerdefinierten MAIL FROM-Domäne \(p. 72\)](#) beschrieben. Als Referenz finden Sie die Feedback-Endpunkte für alle Regionen in der folgenden Tabelle.

Note

Derzeit sind SMTP-Endpunkte in Naher Osten (Bahrain) nicht verfügbar.

Name der Region	Feedback-Endpunkte für benutzerdefinierte „MAIL FROM“-Sendekonfigurationen
US East (Ohio)	feedback-smtp.us-east-2.amazonaws.com
US East (N. Virginia)	feedback-smtp.us-east-1.amazonaws.com
US West (N. California)	feedback-smtp.us-west-1.amazonaws.com
US West (Oregon)	feedback-smtp.us-west-2.amazonaws.com
Asia Pacific (Mumbai)	feedback-smtp.ap-south-1.amazonaws.com
Asia Pacific (Seoul)	feedback-smtp.ap-northeast-2.amazonaws.com
Asia Pacific (Singapore)	feedback-smtp.ap-southeast-1.amazonaws.com

Name der Region	Feedback-Endpunkte für benutzerdefinierte „MAIL FROM“-Sendekonfigurationen
Asia Pacific (Sydney)	feedback-smtp.ap-southeast-2.amazonaws.com
Asia Pacific (Tokyo)	feedback-smtp.ap-northeast-1.amazonaws.com
Canada (Central)	feedback-smtp.ca-central-1.amazonaws.com
Europe (Frankfurt)	feedback-smtp.eu-central-1.amazonaws.com
Europe (Ireland)	feedback-smtp.eu-west-1.amazonaws.com
Europe (London)	feedback-smtp.eu-west-2.amazonaws.com
Europe (Paris)	feedback-smtp.eu-west-3.amazonaws.com
Europe (Stockholm)	feedback-smtp.eu-north-1.amazonaws.com
South America (São Paulo)	feedback-smtp.sa-east-1.amazonaws.com
AWS GovCloud (US)	feedback-smtp.us-gov-west-1.amazonaws.com

Sendeautorisierung

Stellvertretende Absender können nur E-Mails aus der AWS Region senden, in der die Identität des Identitätseigentümers verifiziert ist. Die Richtlinie für die Sendeaufzeichnung, die dem stellvertretenden Sender seine Berechtigung erteilt, muss der Identität in dieser Region angefügt sein. Weitere Informationen zur Sendeaufzeichnung finden Sie unter [Verwenden der Sendeaufzeichnung mit Amazon SES \(p. 162\)](#).

Empfangen von E-Mails

Mit Ausnahme von Amazon S3 Buckets müssen sich alle AWS Ressourcen, die Sie für den Empfang von E-Mails mit Amazon SES verwenden, in derselben AWS-Region wie der Amazon SES -Endpunkt befinden. Wenn Sie z. B. Amazon SES in der Region USA West (Oregon) verwenden, werden alle Amazon SNS Themen, AWS KMSKeys und Lambda Funktionen, die Sie verwenden, müssen sich auch in der Region USA West (Oregon) befinden. Ebenso müssen Sie zum Empfangen von E-Mails mit Amazon SES innerhalb einer Region eine aktive Empfangsregel in dieser Region erstellen.

In der folgenden Tabelle sind die E-Mail-Empfangsendpunkte für alle AWS Regionen aufgeführt, in denen Amazon SES den E-Mail-Empfang unterstützt:

Name der Region	Endpunkte für den E-Mail-Empfang
US East (N. Virginia)	inbound-smtp.us-east-1.amazonaws.com
US West (Oregon)	inbound-smtp.us-west-2.amazonaws.com
Europe (Ireland)	inbound-smtp.eu-west-1.amazonaws.com

Note

Amazon SES unterstützt nicht den E-Mail-Empfang in den folgenden Regionen: USA Ost (Ohio), USA West (Nordkalifornien), Asien-Pazifik (Mumbai), Asien-Pazifik (Seoul), Asien-Pazifik

(Singapur), Asien-Pazifik (Sydney), Kanada (Mitte), Europa (London), Europa (Paris), Europa (Stockholm), Naher Osten (Bahrain), Südamerika (São Paulo) und AWS GovCloud (US) .

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 Eligible for Increase (Erhöhungsberechtigt) in jedem Abschnitt.

E-Mail-Sendekontingente

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

Sendequote

Note

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

Ressource	Standardkontingent	Zur Erhöhung berechtigt?
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 Anwendungsfall. Note Dieser Wert wurde in der Vergangenheit als „Sendekontingent“ bezeichnet.	Ja (p. 159)
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 Anwendungsfall.	Ja (p. 159)

Nachrichtenkontingente

Ressource	Standardkontingent	Zur Erhöhung berechtigt?
Maximale Nachrichtengröße (einschließlich Anhängen)	10 MB pro Nachricht (nach Base64-Kodierung).	Nein

Kontingente für Sender und Empfänger

Ressource	Standardkontingent	Zur Erhöhung berechtigt?
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 Ein-IdentitätEine Domäne oder E-Mail-Adresse, die Sie zum Senden von E-Mails über Amazon SES verwenden.	Nein

Kontingente für die Ereignisveröffentlichung

Ressource	Standardkontingent	Zur Erhöhung berechtigt?
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 Ereignisziel	10	Nein

Kontingente für E-Mail-Vorlagen

Ressource	Standardkontingent	Zur Erhöhung berechtigt?
Maximale Anzahl von E-Mail-Vorlagen in jeder AWS Region	10.000	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 für den Empfang von E-Mails über Amazon SES aufgeführt.

Ressource	Standardkontingent	Zur Erhöhung berechtigt?
Maximale Anzahl von Regeln pro Empfangsregelsatz	200	Nein
Maximale Anzahl von Aktionen pro Empfangsregel	10	Nein
Maximale Anzahl von Empfängern pro Empfangsregel	100	Nein
Maximale Anzahl der Empfangsregelsätze 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.	30 MB	Nein

Ressource	Standardkontingent	Zur Erhöhung berechtigt?
Maximale E-Mail-Größe (einschließlich Header), die mit einer Amazon SNS Benachrichtigung veröffentlicht werden kann.	150 KB	Nein

Allgemeine Kontingente

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

Amazon SES API-Kontingente

Ressource	Standardkontingent	Zur Erhöhung berechtigt?
Rate, mit der Sie Amazon SES - API-Aktionen aufrufen können.	Alle Aktionen (mit Ausnahme von <code>SendEmail</code> und <code>SendRawEmail</code>) werden auf eine Anforderung pro Sekunde gedrosselt. Weitere Informationen zur Amazon SES API finden Sie im Amazon Simple Email Service API-Referenz .	Nein

Bewährte Methoden für das Versenden von Amazon SES mit

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 \(p. 503\)](#)
- [Tipps und bewährte Methoden \(p. 506\)](#)

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:

- [Bounces \(p. 503\)](#)
- [Complaints \(p. 504\)](#)
- [Nachrichtenqualität \(p. 505\)](#)

Bounces

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 behandelt eine zeitweilige Unzustellbarkeit, indem es versucht, 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 permanente unzustellbaren E-Mails unter 5% zu halten. Je weniger permanente unzustellbare E-Mails es in Ihrem E-Mail-Programm gibt, desto wahrscheinlicher ist es, dass ISPs Ihre

Nachrichten als legitim und wertvoll ansehen. Diese Rate sollte als ein vernünftiges und erreichbares Ziel betrachtet werden, ist aber keine universelle Regel für alle 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 permanente 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 Reputation des Absenders 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 Reputation beim ISP des Empfängers.
- Stellen Sie sicher, dass die Adresse, die Sie verwenden, um Unzustellbarkeitsbenachrichtigungen zu erhalten, E-Mails empfangen kann. Weitere Informationen zum Einrichten von Unzustellbarkeits- und Beschwerdebenachrichtigungen finden Sie unter [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen](#) (p. 288).
- Wenn Ihre eingehende E-Mail von einem ISP zu Ihnen gelangt, anstatt über Ihre eigenen internen Server, kann eine hohe Menge von Unzustellbarkeitsbenachrichtigungen 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 Unzustellbarkeitsbenachrichtigungen 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 [Header-Felder](#) (p. 554).

Complaints

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 ISPs werden Sie benachrichtigen, wenn eine Beschwerde gemeldet wird. Dies wird als Feedback-Schleife aus. Amazon SES leitet Beschwerden von ISPs, die Feedback-Schleifen anbieten, 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 es in Ihrem E-Mail-Programm gibt, desto wahrscheinlicher ist es, dass ISPs Ihre Nachrichten als legitim und wertvoll

ansehen. Diese Rate sollte als ein vernünftiges und erreichbares Ziel betrachtet werden, ist aber keine universelle Regel für alle 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 [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen](#) (p. 288).
- 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 Unzustellbarkeitsbenachrichtigungen, 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 [ReturnPath](#) oder [Litmus](#) können dabei helfen, Inhalte in Ihrer E-Mail zu identifizieren, die Inhaltsfilter auslösen können.
- Enthält Ihre E-Mail Links, überprüfen Sie die URLs für diese Links anhand von DNS-basierten Blackhole-Listen (DNSBLs) wie z.B. [Uribl.com](#) und [Surbl.org](#) aus.
- Vermeiden Sie die Verwendung von Linkverkürzern. Böswillige Absender können Linkverkürzungen verwenden, um das tatsächliche Ziel eines Links zu verbergen. Wenn ISPs merken, dass Linkverkürzungsdienste — selbst die seriösesten — für negative Zwecke genutzt werden, können sie den Zugriff auf diese Dienste insgesamt verweigern. Enthält Ihre E-Mail einen Link zu einem Link, 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.

Tipps und bewährte Methoden

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. Die folgenden Abschnitte enthalten Empfehlungen, mit denen Sie sicherstellen können, dass Ihre E-Mail-Kommunikation Ihr Zielpublikum erreicht.

Allgemeine Empfehlungen

- Versetzen Sie sich in die Lage Ihrer Kunden. Fragen Sie sich selbst, ob Sie die Nachricht selbst erhalten möchten. Wenn die Antwort nicht eindeutig "Ja" lautet, dann sollten Sie die E-Mail wahrscheinlich nicht senden.
- Einige Branchen haben einen schlechten Ruf in Bezug auf die Qualität oder sogar auf schädliche E-Mail-Praktiken. Wenn Sie in den folgenden Branchen tätig sind, müssen Sie Ihre Reputation sehr genau beobachten und Probleme sofort lösen:
 - Hypotheken
 - Darlehen
 - Medikamente und Nahrungsergänzungsmittel
 - Alkohol und Tabak
 - Erwachsenenunterhaltung
 - Casinos und Glücksspiel
 - Heimarbeit

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. Zusätzlich assoziieren einige ISPs Ihre Reputation mit Ihrer "From"-Adresse.
- 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. Einen korrekten und aktuellen WHOIS-Eintrag zu pflegen,

zeigt, dass Sie Transparenz schätzen und ermöglicht es den Nutzern, schnell zu erkennen, ob Ihre Domäne 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.

Authentication

- Authentifizieren Sie Ihre Domäne mit [SPF \(p. 141\)](#) 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 \(p. 142\)](#). 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 verursachte 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.

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 E-Mail-Adressen und Domänen](#) (p. 509).
- Lösungen für Probleme im Zusammenhang mit DKIM finden Sie unter [Beheben von DKIM-Problemen in Amazon SES](#) (p. 511).
- Eine Liste häufiger Zustellungsprobleme, die auftreten können, wenn Sie E-Mails versenden, sowie Abhilfemaßnahmen, die Sie ausführen können, finden Sie unter [Amazon SES Probleme](#) (p. 513).
- Eine Beschreibung der Probleme, die Empfängern möglicherweise angezeigt werden, wenn sie eine E-Mail-Nachricht erhalten, die über Amazon SES gesendet wurde, finden Sie unter [Probleme mit E-Mails von Amazon SES](#) (p. 513) aus.
- Lösungen für Probleme mit Unzustellbarkeits-, Beschwerde- und Zustellungsbenachrichtigungen finden Sie unter [Amazon SES Benachrichtigungsprobleme](#) (p. 514).
- Eine Liste der Fehler, die auftreten können, wenn Sie eine E-Mail-Nachricht mit Amazon SES senden, finden Sie unter [Fehler beim Senden von Amazon SES E-Mails über](#) (p. 515) aus.
- 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](#) (p. 517) aus.
- 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 [Amazon SES SMTP-Probleme](#) (p. 518) aus.
- Eine Liste der Fehlercodes, die von der Amazon SES -Abfrage-API (HTTPS) zurückgegeben werden, finden Sie unter [Von der Amazon SES API zurückgegebene Fehlercodes](#) (p. 448) aus.
- Eine Beschreibung häufiger Probleme im Zusammenhang mit unserer Sendeprüfung und deren Behandlung finden Sie unter [Amazon SES prüfverfahren — Häufig gestellte Fragen](#) (p. 529).
- Informationen darüber, wie DNS-basierte Blackhole Lists (DNSBLs) das Senden von Amazon SES beeinflussen, finden Sie unter [DNS-Blackhole-Liste \(DNSBL\) — Häufig gestellte Fragen](#) (p. 546) aus.

Wenn Sie die Amazon SES -API direkt aufrufen, finden Sie unter [Amazon Simple Email Service API-Referenz](#) für die HTTP-Fehler, die Sie möglicherweise erhalten.

Allgemeine Probleme bei Amazon SES

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 angesiedeten Rechenzentren zugreifen, nutzt Amazon SES ein verteiltes Computing-Modell namens [Letztendliche Datenkonsistenz](#) aus. Jede Änderung, die Sie in Amazon SES (oder anderen AWS -Services) vornehmen, ist erst nach einer bestimmten Zeit in allen möglichen

Endpunkten sichtbar. 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](#) (p. 278)), kann eine kurze Verzögerung auftreten, und zwar zwischen dem Zeitpunkt der Erstellung oder Änderung und dem Zeitpunkt der Aktivierung dieser Änderungen.
- Ereignisziele erstellen und ändern— Wenn Sie ein Ereignisziel erstellen oder ändern (z. B., [um Amazon SES mitzuteilen, dass Ihre E-Mail Daten an einen anderen AWS -Service sendet](#) (p. 313)), kann es zu Verzögerungen kommen, und zwar zwischen dem Zeitpunkt der Erstellung oder Änderung des Ereignisziels und dem Zeitpunkt des tatsächlichen Eintreffens des E-Mail-Sendeereignisses am angegebenen Ziel.

Probleme bei der Verifizierung von E-Mail-Adressen und Domänen

Um eine E-Mail-Adresse oder Domäne mit Amazon SES zu überprüfen, starten Sie den Prozess entweder über die Amazon SES Konsole oder die Amazon SES API. Dieser Abschnitt enthält Informationen, die helfen können, Probleme mit der Verifizierung zu lösen.

Häufige Probleme bei der E-Mail-Verifizierung

- Die Bestätigungs-E-Mail ist nicht angekommen— Wenn Sie die Verfahren in [Amazon Verifizieren von E-Mail-Adressen in Amazon SES](#) (p. 52) Sie erhalten die Verifizierungs-E-Mail nicht innerhalb weniger Minuten, 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.
 - Check [Liste verifizierter Adressen in der Amazon SES Konsole](#). Stellen Sie sicher, dass die E-Mail-Adresse, die Sie verifizieren möchten, fehlerfrei ist.

Häufige Probleme mit der Domänenverifizierung

Wenn Sie versuchen, eine Domäne mit dem in [Überprüfen von Domänen in Amazon SES](#) (p. 65) beschriebenen Verfahren zu verifizieren, und Probleme auftreten, prüfen Sie die möglichen Ursachen und folgenden Lösungen.

- Sie versuchen, eine Domäne zu überprüfen, 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 imgmail.com-Domäne verwenden, müssen Sie [Überprüfen Sie, ob die E-Mail-Adresse speziell](#) (p. 52). Sie können nicht die gesamte Domäne gmail.com verifizieren.
- Ihr DNS-Anbieter erlaubt keine Unterstriche in TXT-Datensatznamen— Einige DNS-Anbieter lassen nicht zu, dass Sie den Unterstrich in die DNS-Datensatznamen für Ihre Domäne einschließen. Wenn diese Bedingung auf "true" gesetzt ist, können Sie _amazonses im Namen des TXT-Datensatzes weglassen.
- Ihr DNS-Anbieter hat den Domännennamen an das Ende des TXT-Datensatzes angehängt— Einige DNS-Anbieter hängen den Namen Ihrer Domäne automatisch an den Attributnamen des TXT-Datensatzes an. Wenn Sie z. B. einen Datensatz mit dem Attributnamen _amazonses.example.com erstellen, hängt der

Anbieter möglicherweise den Domänennamen an, woraus sich `_amazonses.example.com.example.com` ergibt. Zur Vermeidung doppelter Domänennamen können an das Ende des Domänennamens einen Punkt anfügen, wenn Sie den TXT-Datensatz erstellen. Dieser Schritt gibt Ihrem DNS-Anbieter zu verstehen, dass es nicht erforderlich ist, den Domänennamen an den TXT-Datensatz anzuhängen.

- Ihr DNS-Anbieter hat den DNS-Datensatzwert geändertEinige Anbieter ändern automatisch DNS-Datensatzwerte, um nur Kleinbuchstaben zu verwenden. Amazon SES verifiziert Ihre Domäne nur, wenn ein Verifizierungsdatensatz erkannt wird, für den der Attributwert genau mit dem Wert übereinstimmt, den Amazon SES beim Start der Domänenverifizierung angegeben hat. Wenn der DNS-Anbieter für Ihre Domäne Ihre TXT-Datensatzwerte in ausschließlich Kleinbuchstaben ändert, wenden Sie sich an den DNS-Anbieter für zusätzliche Unterstützung.
- Sie möchten dieselbe Domäne mehrmals überprüfenMöglicherweise müssen Sie Ihre Domäne mehrmals überprüfen, weil Sie in verschiedenen Regionen senden oder weil Sie dieselbe Domäne für das Senden von mehreren AWS Konten verwenden. Wenn Ihr DNS-Anbieter nicht mehr als einen TXT-Datensatz mit demselben Attributnamen zulässt, können Sie möglicherweise dennoch zwei Domänen verifizieren. Falls Ihr DNS-Anbieter dies zulässt, können Sie demselben TXT-Datensatz mehrere Attributwerte zuweisen. Wenn Ihr DNS von Amazon Route 53 verwaltet wird, können Sie mit dem folgenden Verfahren mehrere Werte für denselben TXT-Datensatz einrichten:
 1. Wählen Sie in der Route 53 Konsole den TXT-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 Ihnen nicht gestattet, demselben TXT-Datensatz mehrere Werte zuzuweisen, können Sie die Domäne einmal mit `_amazonses` im Attributnamen des TXT-Datensatzes und ein weiteres Mal ohne `_amazonses` 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 TXT-Datensatz zur - 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`.

In diesem Verfahren müssen Sie zunächst die für Ihre Domäne zuständigen DNS-Server suchen und anschließend diese Server abfragen, um die TXT-Datensätze angezeigt zu bekommen. Sie fragen die für Ihre Domäne zuständigen DNS-Server ab, da diese die neuesten Informationen für Ihre Domäne enthalten. Die Verteilung dieser Informationen an andere DNS-Server kann einige Zeit in Anspruch nehmen.

So überprüfen Sie, ob Ihr TXT-Datensatz für die Domänenverifizierung auf Ihrem DNS-Server veröffentlicht wird

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. Überprüfen Sie anhand der folgenden Schritte, ob der TXT-Datensatz korrekt veröffentlicht wurde.

- a. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein. Dabei ist <domain> Ihre Domäne und <name server> einer der Nameserver, die Sie in Schritt 1 ermittelt haben.

```
nslookup -type=TXT _amazonses.<domain> <name server>
```

Wenn in unserem ses-example.com-Beispiel in Schritt 1 ein Nameserver mit dem Namen ns1.name-server.net gefunden wurde, geben Sie also Folgendes ein:

```
nslookup -type=TXT _amazonses.ses-example.com ns1.name-server.net
```

- b. Überprüfen Sie in der Ausgabe des Befehls, ob die Zeichenfolge `nachtext` = entspricht dem TXT-Wert, der beim Auswählen der Domäne in der Liste „Identities (Identitäten)“ in der Amazon SES-Konsole angezeigt wird.

In diesem Beispiel suchen wir unter `_amazonses.ses-example.com` einen TXT-Datensatz mit dem Wert `fmqxqT/icOYx4aA/bEUrDPMeax9/s3frb1S+niixmqk=`. Wenn der Datensatz ordnungsgemäß veröffentlicht wurde, wird folgende Befehlsausgabe erwartet:

```
_amazonses.ses-example.com text = "fmqxqT/icOYx4aA/bEUrDPMeax9/s3frb1S+niixmqk="
```

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](#) (p. 143) oder [BYODKIM](#) (p. 150) 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. Wenn Sie DKIM für eine Identität in der Amazon SES Konsole aktivieren möchten, wählen Sie die E-Mail-Domäne in der Identitäten-Liste. 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 mehreren AWS Regionen verwenden, müssen Sie DKIM für jede Region einzeln konfigurieren. Wenn Sie dieselbe Domäne mit mehreren AWS Konten verwenden, müssen Sie DKIM gleichermaßen für jedes Konto konfigurieren. 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 Ihnen Amazon SES eine Benachrichtigung per E-Mail.

Die DKIM-Details Ihrer Domäne werden in der Amazon SES Konsole angezeigt. DKIM: Warten auf Sender-Verifizierung... DKIM-Verifizierungsstatus: Überprüfung ausstehend

Wenn Sie die Prozeduren in [Easy DKIM \(p. 143\)](#) oder [Bereitstellen Ihres eigenen DKIM-Authentifizierungs-Tokens \(p. 150\)](#) Wenn Sie DKIM für eine Domäne konfigurieren möchten, 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-Einträge 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 Domännennamen 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 aufweisen und 1024-Bit-RSA-Verschlüsselung verwenden. Darüber hinaus muss der private Schlüssel base64-codiert sein.

Beim Einrichten von BYODKIM erhalten Sie eine **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 Amazon SES DKIM CNAME-Einträge zurück, geben jedoch **SERVFAIL** für den TXT-Eintrag zur Domänenüberprüfung.

Ihr DNS-Anbieter kann CNAME-Einträge möglicherweise nicht umleiten. Amazon SES und ISPs fragen TXT-Datensätze ab. 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 enthält `amazonses.com`, wird automatisch von Amazon SES hinzugefügt. Sie können sie ignorieren.

Amazon SES Probleme

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 die [AWS Service Health Dashboard](#). Überprüfen Sie und vergewissern Sie sich, 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. Stellen Sie uns bitte in Ihrer Korrespondenz alle relevanten Empfängeradressen sowie Anforderungs- oder Mitteilungs-IDs zur Verfügung, die in den `SendEmail`- oder `SendRawEmail`-Antworten zurückgegeben werden.
- Warten Sie, um zu sehen, ob das Problem tatsächlich eine Verzögerung und nicht eine dauerhafte Unzustellbarkeit ist. Im Kampf gegen Spammer lehnen einige ISPs eingehende Nachrichten von unbekannten E-Mail-Ausgangsservern zeitweise ab. Dieser Prozess, genannt 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.

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 \(p. 142\)](#) (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 \(p. 142\)](#).

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 die MIME-Nachricht erstellt haben, können Sie sie mit der [SendRawEmail-API](#) senden. Weitere Informationen über das Senden von Nachrichten mit der SendRawEmail -API finden Sie unter [Senden von Raw-E-Mails mit den AWS -SDKs \(p. 478\)](#) aus.

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 können 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 vorhergehenden Absatz verwenden. Informationen zur Deaktivierung dieser Funktion finden Sie unter [Intelligente Anführungszeichen in Word](#) auf der Microsoft Office-Support-Website.

Amazon SES Benachrichtigungsprobleme

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:
 - Speichern Sie in Amazon SES, die Sie hinzugefügt haben, eine Zuordnung zwischen einer Kennung und der Amazon SES Mitteilungs-ID, die Amazon SES zurückgibt, wenn die E-Mail akzeptiert wird.
 - 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 Beschwerdebenachrichtigungen über Amazon SNS oder Weiterleitungen von Feedback per E-Mail, wissen aber nicht, auf welche Empfänger sich diese Benachrichtigungen beziehen— Einige ISPs bearbeiten die E-Mail-Adresse des beschwerenden Empfängers, bevor sie die Beschwerdebenachrichtigung an Amazon SES übermitteln. Damit Sie die E-Mail-Adresse des

Empfängers finden können, empfiehlt sich eine Speicherung Ihrer eigenen Zuordnung zwischen einer Kennung und der Amazon SES Mitteilungs-ID, die Amazon SES zurückgibt, wenn die E-Mail akzeptiert wird. Beachten Sie, dass Amazon SES keine benutzerdefinierte Mitteilungs-IDs speichert, die Sie hinzufügen.

- Sie möchten Benachrichtigungen einrichten, um zu einem Amazon SNS -Thema zu gelangen, das Sie nicht besitzen— Der Eigentümer des Themas muss eine Amazon SNS Zugriffsrichtlinie konfigurieren, die Ihr Konto berechtigt, die `SNS:Publish`-Aktion zu ihrem Thema. Weitere Informationen darüber, wie Sie den Zugriff auf Ihr Amazon SNS -Thema mithilfe von IAM-Richtlinien kontrollieren, finden Sie unter [Verwalten des Zugriffs auf Ihre Amazon SNS -Themen](#) in der Amazon Simple Notification Service-Entwicklerhandbuchaus.

Fehler beim Senden von Amazon SES E-Mails über

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, die in der [Häufige Fehler](#)-Thema des Amazon Simple Email Service API-Referenz aus.
- 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. Beispielsweise kann die Ausnahme eine `AmazonSESMessageRejectedException` (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 \(p. 519\)](#) aus.

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 sind zusätzlich zu allgemeinen AWS Fehlern wie `MalformedQueryString`, wie in der [Häufige Fehler](#)-Thema des Amazon Simple Email Service API-Referenz aus.

- Email address is not verified. The identities failed the check in region: `Identität1, Identität2, Identität3`— Sie versuchen, E-Mails von einer E-Mail-Adresse oder Domäne zu senden, die nicht über [Verifiziert mit Amazon SES \(p. 52\)](#) aus. Dieser Fehler kann für folgende Adressen gelten: "From", "Source", "Sender" oder "Return-Path". Wenn Ihr Konto noch in [Amazon SES Sandbox \(p. 79\)](#) verfügen, müssen Sie alle E-Mail-Adressen aller Empfänger verifizieren. Dies gilt nicht für Empfänger, die vom [Amazon SES Postfachsimulator \(p. 198\)](#) aus. Wenn Amazon SES nicht alle fehlgeschlagenen Identitäten auflisten kann, endet die Fehlermeldung mit Auslassungspunkten.

Note

Amazon SES verfügt über Endpunkte in [Mehrere AWS Regionen \(p. 494\)](#). Die Verifizierung des Status von E-Mail-Adressen erfolgt für jede AWS Region separat. Sie müssen den

Verifizierungsprozess für jeden Sender in einer AWS Region durchführen, den Sie verwenden möchten.

- Konto ist angehalten— Die Fähigkeit Ihres Kontos, E-Mails zu senden, wurde unterbrochen. 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 Ihres Kontos zum Versenden von E-Mails unterbrechen, senden wir automatisch eine Benachrichtigung an die E-Mail-Adresse, die mit Ihrem AWS Konto verknüpft ist. Weitere Informationen finden Sie unter [the section called "Überprüfen" \(p. 529\)](#).

- Drosselung— Ihre Anwendung versucht möglicherweise, zu viele Nachrichten pro Sekunde zu senden oder Sie haben in den letzten 24 Stunden zu viele E-Mails gesendet. In diesen Fällen kann die Fehlermeldung den folgenden Beispielen ähneln:
 - Daily message quota exceeded— Sie haben die maximale Anzahl von Nachrichten gesendet, die innerhalb von 24 Stunden erlaubt sind. Wenn Sie Ihr tägliches Kontingent überschritten haben, müssen Sie bis zum nächsten 24-Stunden-Zeitraum warten, bevor Sie weitere E-Mails senden können.
 - Maximum sending rate exceeded— Sie versuchen, mehr E-Mails pro Sekunde zu senden, als von Ihrer maximalen Senderate erlaubt. Wenn Sie Ihre Senderate überschritten haben, können Sie weiterhin E-Mails senden, müssen jedoch die Senderate reduzieren. Weitere Informationen finden Sie unter [Beheben Sie einen Fehler „Throttling - Maximum send rate exceeded“ \(Maximum send rate exceeded\)](#) im AWS Messaging and Targeting Blog.
 - Maximale SigV2-SMTP-Senderate 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 AWS-Signatur erstellt. Aus Sicherheitsgründen sollten Sie Anmeldeinformationen löschen, die vor diesem Datum erstellt wurden, und sie durch neuere Anmeldeinformationen ersetzen. Sie können ältere Anmeldeinformationen mit der IAM-Konsole löschen. Weitere Informationen finden Sie unter [the section called "Abrufen Ihrer - SMTP-Anmeldeinformationen" \(p. 95\)](#) zum Erstellen von Anmeldeinformationen.

Sie sollten Ihre Sendeaktivitäten regelmäßig überwachen, um Ihre Sendekontingente im Auge zu behalten. Weitere Informationen finden Sie unter [Überwachen Ihrer Amazon SES Versandkontingente \(p. 158\)](#). Allgemeine Informationen zu Sendekontingenten finden Sie unter [Verwalten Ihrer Amazon SES Versandkontingente \(p. 156\)](#). Weitere Informationen zum Erhöhen Ihrer Sendekontingente finden Sie unter [Erhöhen Ihrer Amazon SES Versandkontingente \(p. 159\)](#).

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 zu den Service-Status finden Sie unter [AWS Service Health Dashboard](#) aus.

- There are no recipients specified – Es wurden keine Empfänger angegeben.
- In der E-Mail-Adresse sind Nicht-ASCII-Zeichen vorhanden— 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 Raw-E-Mails mithilfe der Amazon SES API \(p. 121\)](#) beschrieben kodieren. Weitere Informationen zu Punycode finden Sie unter [RFC 3492](#).
- Mail FROM Domain ist nicht verifiziert— Amazon SES konnte den MX-Datensatz nicht lesen, der für die Verwendung der angegebenen MAIL FROM-Domäne erforderlich ist. Weitere Informationen zum Einrichten benutzerdefinierter MAIL FROM-Domänen finden Sie unter [Einrichten einer benutzerdefinierten MAIL FROM-Domäne \(p. 72\)](#).
- 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 mit Amazon SES Ereignisveröffentlichung \(p. 313\)](#).

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](#) (p. 156).) Allerdings benötigt jeder Aufruf an Amazon SES Zeit für die Ausführung.

Wenn Sie mehrere -Aufrufe an Amazon SES 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 identifizieren— 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 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.
- Verwenden Sie mehrere Threads— 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 E/A-intensive Operation. Mit dem Einsatz mehrerer Threads wird ein höherer Durchsatz erzielt. Sie können gleichzeitig senden und dabei beliebig viele Ausführungs-Threads verwenden.
- Erwägen Sie die Verwendung mehrerer Prozesse— Die Verwendung mehrerer Prozesse kann dazu beitragen, Ihren 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.
- Erwägen Sie die Verwendung eines lokalen E-Mail-Relays— 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](#) (p. 102).
- Erwägen Sie, Ihre Anwendung näher am Amazon SES API-Endpunkt zu hosten— Vielleicht sollten Sie Ihre Anwendung in einem Rechenzentrum in der Nähe des Amazon SES API-Endpunkts oder auf einer Amazon EC2 Instance in derselben AWS Region wie der Amazon SES API-Endpunkt 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 erhältlich ist, finden Sie unter [Amazon Simple Email Service \(Amazon SES\)](#) in der Allgemeinen AWS-Referenzaus.
- Erwägen Sie die Verwendung mehrerer Maschinen— 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.
- Erwägen Sie, die Amazon SES Abfrage-API anstelle des SMTP-Endpunkts zu verwenden— Die Verwendung der Amazon SES -Abfrage-API ermöglicht es Ihnen, die E-Mail-Sendeanforderung mithilfe eines einzelnen Netzwerkaufrufs zu senden, während die Verbindung mit dem SMTP-Endpunkt eine SMTP-Konversation beinhaltet, die aus mehreren Netzwerk-Anfragen 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](#) (p. 120) aus.

- Verwenden Sie den Amazon SES -Postfachsimulator, um Ihren maximalen Durchsatz zu testen— Um Änderungen zu testen, die Sie implementieren möchten, können Sie den -Postfachsimulator verwenden. 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 [Testen der E-Mail-Versendung in Amazon SES \(p. 198\)](#).

Wenn Sie auf Amazon SES über die SMTP-Schnittstelle zugreifen, erhalten Sie unter weitere Informationen unter [Amazon SES SMTP-Probleme \(p. 518\)](#) Für bestimmte SMTP-bezogene Probleme, die den Durchsatz beeinflussen können.

Amazon SES SMTP-Probleme

Dieser Abschnitt enthält Lösungen für mehrere häufig auftretende Probleme im Zusammenhang mit dem Senden von E-Mails Amazon SES -SMTP-Schnittstelle (Simple Mail Transfer Protocol). Er enthält auch eine Liste der von Amazon SES zurückgegebenen SMTP-Antwortcodes.

Weitere Informationen zum Senden von E-Mails über die -SMTP-Schnittstelle von Amazon SES finden Sie unter [Senden von E-Mails über die Amazon SES SMTP-Schnittstelle \(p. 94\)](#).

- 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 verwenden, um eine Verbindung mit dem -SMTP-Endpunkt herzustellen, unterscheiden sich von Ihren AWS Anmeldeinformationen. Informationen zum Abrufen Ihrer SMTP-Anmeldeinformationen finden Sie unter [Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen \(p. 95\)](#). Weitere Informationen zu Anmeldeinformationen finden Sie unter [Arten von Amazon SES Anmeldeinformationen \(p. 18\)](#).
- Netzwerk- oder Firewall-ProblemeMöglicherweise 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 gezeigten Verfahren durch. [Testen der Verbindung zur Amazon SES SMTP-Schnittstelle über die Befehlszeile \(p. 113\)](#).

Wenn Sie keine Verbindung zum -Amazon SES SMTP-Endpunkt über `telnet` oder `openssl` Es ist 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 Request to Remove Email Sending Limitations](#) (. 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 MTU (Maximum Transmission Unit, MTU) der Netzwerkschnittstelle für den Computer, mit dem Sie eine Verbindung mit der Amazon SES -SMTP-Schnittstelle herstellen, ist möglicherweise 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 im Client zu hängen und erreichen den Cluster nicht](#) im Amazon Redshift Clusterverwaltungshandbuch.

Weitere Informationen über das Festlegen der MTU-Größe für eine Amazon EC2 Instance finden Sie unter [Netzwerk-MTU \(Maximum Transmission Unit\) für Ihre EC2 Instance](#) im Amazon EC2-Benutzerhandbuch für Linux-Instances.

- 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 aktuell und fehlertolerant ist, werden aktive Amazon 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 -SMTP-E-Mail-Server von Amazon SES wissen, damit Sie die IP-Adressen in eine weiße Liste für Ihr Netzwerk eintragen können.

Die IP-Adressen für die -Amazon SES SMTP-Endpunkte befinden sich hinter Load Balancern. Infolgedessen ändern sich diese IP-Adressen häufig. Es ist nicht möglich, eine endgültige Liste aller IP-Adressen für die Amazon SES Endpunkte bereitzustellen. Es wird empfohlen, die `amazonses.com`-Domäne auf die Whitelist zu setzen, anstatt einzelne IP-Adressen auf die Whitelist zu setzen.

Von Amazon SES zurückgegebene SMTP-Antwortcodes

Dieser Abschnitt enthält eine Liste der von der -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 unter [How to handle a „Throttling - Maximum sending rate exceeded“ error](#) im AWS Messaging and Targeting Blog.

Note

AWS SDKs implementieren die Logik für Wiederholversuche [Automatisch](#). Sie verwenden aber 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 beispielsweise Ihre AWS-Anmeldeinformationen für die

AWS-Authentifizierung ungültig sind, müssen Sie Ihre Anwendung dahingehend aktualisieren, dass die richtigen Anmeldeinformationen verwendet werden, bevor Sie die Anforderung erneut senden.

Beschreibung	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 <i>MessageID</i>	<i>MitteilungsID</i> Eine eindeutige Zeichenfolge, die Amazon SES zur eindeutigen Identifizierung einer Nachricht verwendet.
Service nicht verfügbar	421 Too many concurrent SMTP connections	Amazon SES kann die Anforderung nicht verarbeiten, weil zurzeit zu viele Verbindungen zum SMTP-Server hergestellt sind.
Lokaler Verarbeitungsfehler	451 Temporary service failure	Amazon SES konnte die Anforderung nicht verarbeiten. Mit der Anforderung gibt es möglicherweise Probleme, die die Verarbeitung verhindern.
Timeout	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 (p. 156) .
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 (p. 156) .
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 Ihrem E-Mail-Programm und Amazon SES vor. Beachten Sie, dass Sie eine verschlüsselte Verbindung verwenden müssen,

Beschreibung	Antwortcode	Weitere Informationen
		wenn Sie eine Verbindung mit Amazon SES herstellen. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem Amazon SES SMTP-Endpunkt (p. 100). In Amazon SES kann ein Problem auftreten. Überprüfen Sie die AWS Service Health Dashboard für Aktualisierungen.
Probleme mit dem Eingang der Anforderung	454 Temporary service failure	Amazon SES hat 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 Herstellen einer Verbindung mit der -SAmazon SES TP-Schnittstelle nicht versucht.
Ungültige Anmeldeinformationen für die Authentifizierung	535 Authentication Credentials Invalid	Die Anwendung, die Sie zum Senden von E-Mails verwenden, hat Amazon SES nicht die richtigen SMTP-Anmeldeinformationen bereitgestellt. Beachten Sie, dass Ihre Anmeldeinformationen für SMTP und AWS nicht identisch sind. Weitere Informationen finden Sie unter Abrufen Ihrer Amazon SES SMTP-Anmeldeinformationen (p. 95).
Amazon SES hat Amazon SES nicht abonniert	535 Account not subscribed to SES	Das AWS Konto als Eigentümer der SMTP-Anmeldeinformationen ist für Amazon SES nicht registriert.
Nachricht ist zu lang	552 Message is too long.	Die Nachricht, die Sie senden möchten, ist größer als 10 MB.
Amazon SES hat Amazon SES nicht abonniert	535 Account not subscribed to SES	Das AWS Konto als Eigentümer der SMTP-Anmeldeinformationen ist für Amazon SES nicht registriert.
Benutzer zum Aufrufen des Amazon SES SMTP-Endpunkts nicht autorisiert	554 Access denied: User <i>UserARN</i> is not authorized to perform ses:SendRawEmail on resource <i>IdentityARN</i>	Die AWS Identity and Access Management (IAM) -Richtlinie oder die Amazon SES Sendeautorisierung des Benutzers, der Eigentümer der SMTP-Anmeldeinformationen ist, hat keine Erlaubnis, den Amazon SES SMTP-Endpunkt aufzurufen.

Beschreibung	Antwortcode	Weitere Informationen
Nicht verifizierte E-Mail-Adresse	554 Message rejected: Email address is not verified. The following identities failed the check in region <i>region</i> : <i>identity0</i> , <i>identity1</i> , <i>identity2</i>	Sie versuchen, eine E-Mail von einer E-Mail-Adresse oder Domäne zu senden, die nicht Verifiziert, um E-Mails von Ihrem Amazon SES Konto zu senden (p. 52). 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 SES Postfachsimulator (p. 198)) enthalten. Wenn Amazon SES nicht alle bei der Verifizierung fehlgeschlagenen Identitäten anzeigen kann, endet die Fehlermeldung mit drei Punkten (...). Note Amazon SES verfügt über Endpunkte in Mehrere AWS Regionen (p. 494). Der Verifizierungsstatus von E-Mail-Adressen ist für jede AWS Region separat. Sie müssen den Verifizierungsprozess für jeden Sender in AWS Regionen durchführen, den Sie verwenden möchten.

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 dauerhaft löschen.

Dieses Kapitel enthält Verfahren zum Löschen verschiedener Arten von Daten, die als personenbezogen angesehen werden könnten.

Themen in diesem Abschnitt:

- [Löschen von E-Mail-Adressen aus der Unterdrückungsliste auf Kontoebene \(p. 523\)](#)
- [Löschen von Daten zu mit Amazon SES gesendeten E-Mails \(p. 524\)](#)
- [Löschen von Daten über Identitäten \(p. 525\)](#)
- [Löschen von Absender-Authentifizierungsdaten \(p. 525\)](#)
- [Löschen von auf Empfangsregeln bezogenen Daten \(p. 526\)](#)
- [Löschen von auf IP-Adressfilter bezogenen Daten \(p. 527\)](#)
- [Löschen von Daten in E-Mail-Vorlagen \(p. 527\)](#)
- [Löschen von Daten in benutzerdefinierten Vorlagen zur E-Mail-Verifizierung \(p. 527\)](#)
- [Löschen aller personenbezogenen Daten durch Schließen Ihres AWS Kontos \(p. 528\)](#)

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 \(p. 201\)](#).

E-Mail-Adressen können aus der Unterdrückungsliste auf Kontoebene entfernt werden, indem Sie die `DeleteSuppressedDestination`-Operation im [Amazon SES API v2](#). 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](#).

So entfernen Sie mithilfe der AWS CLI eine Adresse aus der Unterdrückungsliste auf Kontoebene

- 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 von der Unterdrückungsliste auf Kontoebene entfernen möchten.

Löschen von Daten zu mit Amazon SES gesendeten E-Mails

Wenn Sie mit Amazon SES eine E-Mail senden, können Sie Informationen zu dieser E-Mail an andere AWS -Services senden. Beispielsweise können Sie Informationen über E-Mail-Ereignisse (wie z. B. Auslieferungen, Öffnungen und Klicks) an Kinesis Data 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 E-Mail-Ereignisdaten mithilfe von Kinesis Data Firehose an verschiedene Ziele streamen. Es handelt sich dabei um beispielsweise um Amazon Simple Storage Service, Amazon Elasticsearch Service und Amazon Redshift. Um diese Daten zu entfernen, sollten Sie zunächst das Streamen von Daten an Kinesis Data Firehose und dann die bereits gestreamten Daten löschen. Um das Streamen von Amazon SES -Ereignisdaten an Kinesis Data Firehose zu stoppen, müssen Sie das -Ereignisziel von Kinesis Data Firehose löschen.

So entfernen Sie ein Kinesis Data Firehose Ereignisziel über die Amazon SES Konsole

1. Öffnen der Amazon 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 -Ereignisziel von Kinesis Data Firehose enthält.
4. Neben dem zu löschenden Kinesis Data Firehose-Ereignisziel wählen Sie `delete` (Löschen).
5. Falls erforderlich, entfernen Sie die Daten, die Kinesis Data Firehose an andere Services übermittelt hat. Weitere Informationen finden Sie unter [the section called "Entfernen gespeicherter Ereignisdaten"](#) (p. 524).

Ereignisziele können auch mithilfe der Amazon SES -API gelöscht werden. Im folgenden Verfahren wird die AWS Command Line Interface (AWS CLI), um mit der Amazon SES API zu interagieren. Sie können auch über ein AWS S-SDK oder über direkte HTTP-Anfragen mit der API interagieren.

So entfernen Sie ein Kinesis Data Firehose Ereignisziel mithilfe der AWS CLI

1. Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-configuration-set-event-destination --configuration-set-name configSet \
--event-destination-name eventDestination
```

Ersetzen Sie in diesem Befehl *configSet* mit dem Namen des Konfigurationssatzes, der das Kinesis Data Firehose -Ereignisziel enthält. Ersetzen *EventDestination* mit dem Namen des Kinesis Data Firehose Ereignisziels.

2. Falls erforderlich, entfernen Sie die Daten, die Kinesis Data Firehose an andere Services übermittelt hat. Weitere Informationen finden Sie unter [the section called "Entfernen gespeicherter Ereignisdaten"](#) (p. 524).

Entfernen gespeicherter Ereignisdaten

Informationen zum Löschen von Informationen aus anderen AWS-Services können Sie den folgenden Dokumenten entnehmen:

- [Objekt und Bucket löschen](#) im Handbuch „Erste Schritte“ für Amazon Simple Storage Service
- [Löschen einer Amazon ES-Domain](#) im Entwicklerhandbuch zu Amazon Elasticsearch Service

- [Löschen eines Clusters](#) im Clusterverwaltungs-Handbuch von Amazon Redshift

Sie können E-Mail-Daten auch mit Kinesis Data Firehose an Splunk streamen. Es handelt sich dabei um einen Drittanbieterdienst, der von AWS nicht unterstützt wird oder nicht in der AWS Management Console. 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 der Amazon 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 Identity (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), um mit der Amazon SES API zu interagieren. Sie können auch über ein AWS S-SDK oder über direkte HTTP-Anfragen mit der API interagieren.

So löschen Sie eine Identität mithilfe der 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 \(p. 162\)](#) eine Richtlinie erstellen. Diese Richtlinien enthalten Identitäten (die Ihnen gehören) sowie auch AWS IDs (die der Person oder Gruppe zugeordnet sind, von der die E-Mail in Ihrem Auftrag gesendet wird). 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 der Amazon 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. Im folgenden Verfahren wird die AWS Command Line Interface (AWS CLI), um mit der Amazon SES API zu interagieren. Sie können auch über ein AWS S-SDK oder über direkte HTTP-Anfragen mit der API interagieren.

So löschen Sie eine Absender-Authentifizierungsrichtlinie mithilfe der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-identity-policy --identity example.com --policy-name samplePolicy
```

Ersetzen Sie in diesem Befehl *example.com* durch die Identität, in der die Absender-Authentifizierungsrichtlinie enthalten ist. Ersetzen Sie *samplePolicy* durch den Namen der Absender-Authentifizierungsrichtlinie.

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 der Amazon 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. Im folgenden Verfahren wird die AWS Command Line Interface (AWS CLI), um mit der Amazon SES API zu interagieren. Sie können auch über ein AWS S-SDK oder über direkte HTTP-Anfragen mit der API interagieren.

So löschen Sie eine Empfangsregel mithilfe der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-receipt-rule --rule-set myRuleSet --rule-name myReceiptRule
```

Ersetzen Sie in diesem Befehl *myRuleSet* durch den Namen des Empfangsregelsatzes, in dem die Empfangsregel enthalten ist. Ersetzen Sie *myReceiptRule* 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 der Amazon 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. Im folgenden Verfahren wird die AWS Command Line Interface (AWS CLI), um mit der Amazon SES API zu interagieren. Sie können auch über ein AWS S-SDK oder über direkte HTTP-Anfragen mit der API interagieren.

So löschen Sie einen IP-Adressfilter mithilfe der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-receipt-filter --filter-name IPfilter
```

Ersetzen Sie in diesem 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.

So löschen Sie eine E-Mail-Vorlage mithilfe der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-template --template-name sampleTemplate
```

Ersetzen Sie in diesem 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.

So löschen Sie eine benutzerdefinierte Vorlage zur E-Mail-Verifizierung mithilfe der AWS CLI

- Geben Sie in der Befehlszeile folgenden Befehl ein:

```
aws ses delete-custom-verification-email-template --template-  
name verificationEmailTemplate
```

Ersetzen Sie in diesem Befehl *verificationEmailTemplate* durch den Namen der benutzerdefinierten Vorlage zur E-Mail-Verifizierung, die Sie löschen möchten.

Löschen aller personenbezogenen Daten durch Schließen Ihres AWS Kontos

Es ist auch möglich, alle personenbezogenen Daten, die in Amazon SES gespeichert sind, durch Schließen Ihres AWS Kontos zu löschen. Diese Aktion löscht auch alle anderen Daten — personenbezogene und nicht personenbezogene —, die Sie in jedem anderen AWS -Service gespeichert haben.

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.

Warning

Starten Sie erst dann mit dem folgenden Verfahren, wenn Sie sich sicher sind, dass Sie alle in Ihrem AWS und -Regionen gespeicherten Daten vollständig entfernen möchten.

Sie können Ihr AWS Konto über die schließenAWS Management Console.

So schließen Sie Ihr AWS Konto

1. Öffnen Sie AWS Management Consoleum <https://console.aws.amazon.com/>.
2. Rufen Sie auf Kontoeinstellungen-Seite unter <https://console.aws.amazon.com/billing/home?#/account>.

Warning

Die folgenden beiden Schritte werden endgültig gelöscht. Alle Daten, die Sie in allen AWS-Services in allen AWS-Regionen gespeichert haben.

3. **UNTER** Konto schließen Lesen Sie im Haftungsausschluss, der auf die Folgen bei einer Schließung Ihres AWS Kontos eingeht. Wenn Sie den Bedingungen zustimmen, aktivieren Sie das Kontrollkästchen und wählen Sie dann Konto schließen.
4. Klicken Sie im Bestätigungsdialogfeld auf Konto schließen.

Amazon SES fig gestellte Fragen zu

In diesem Abschnitt finden Sie Antworten auf häufig gestellte Fragen zur Nutzung von Amazon SES.

Häufig gestellte Fragen

- [Amazon SES prüfverfahren — Häufig gestellte Fragen \(p. 529\)](#)
- [DNS-Blackhole-Liste \(DNSBL\) — Häufig gestellte Fragen \(p. 546\)](#)
- [Häufig gestellte Fragen zu -E-Mail-Sendemetriken \(p. 549\)](#)

Amazon SES prüfverfahren — Häufig gestellte Fragen

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 \(p. 529\)](#) für das betreffende Konto fest. In anderen Fällen [unterbrechen wir die Fähigkeit des Kontos, E-Mails zu senden \(p. 532\)](#). Wir ergreifen diese Maßnahmen, um die Zuverlässigkeit des Senders eines jeden Kontos zu schützen und für andere Amazon SES Benutzer Service-Unterbrechungen und Probleme mit der Zustellbarkeit zu verhindern.

Dieser Abschnitt enthält häufig gestellte Fragen zu den folgenden Themen:

- [Konto wird geprüft – Häufig gestellte Fragen \(p. 529\)](#)
- [Sendeunterbrechung – Häufig gestellte Fragen \(p. 532\)](#)
- [Unzustellbarkeit – Häufig gestellte Fragen \(p. 534\)](#)
- [Beschwerden – Häufig gestellte Fragen \(p. 537\)](#)
- [Pseudo-E-Mail-Adressen für Spam – Häufig gestellte Fragen \(p. 542\)](#)
- [Manuelle Überprüfung – Häufig gestellte Fragen \(p. 544\)](#)

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 eine Prüfung für Ihr Konto festgelegt ist, wird automatisch eine Benachrichtigung an die E-Mail-Adresse gesendet, die mit Ihrem AWS Konto verknüpft ist. Diese E-Mail-Adresse entspricht der beim Erstellen Ihres AWS Kontos angegebenen Adresse. In einigen Fällen kann diese E-Mail-Adresse von der Adresse abweichen, die Sie zum Senden von E-Mails über Amazon SES verwenden.

Wir empfehlen, dass Sie Ihre Zuverlässigkeit als Absender überwachen, indem Sie regelmäßig auf das [Reputation Dashboard \(p. 400\)](#) zugreifen. Sie können [Einrichten automatischer Alarme in Amazon CloudWatch \(p. 415\)](#). Mithilfe dieser Alarme erhalten Sie eine Benachrichtigung, wenn Ihre Zuverlässigkeitsmetriken bestimmte Grenzwerte überschreiten. Sie können auch andere Möglichkeiten der Kontaktaufnahme für Amazon CloudWatch konfigurieren, z. B. Senden einer SMS-Nachricht an Ihr Mobiltelefon.

F4. Hat die Tatsache, dass mein Amazon SES S-Konto geprüft wird, Auswirkungen auf meine Nutzung anderer AWS -Services?

Sie können weiterhin andere AWS Dienste verwenden, während Ihr Amazon SES S-Konto geprüft wird. Wenn Sie jedoch eine Erhöhung des Servicekontingents für einen anderen AWS S-Service anfordern, der ausgehende Kommunikation sendet (z. B. Amazon SNS), wird dieser Antrag möglicherweise abgelehnt werden, bis der Überprüfungszeitraum Ihres Amazon SES S-Kontos aufgehoben ist.

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.
- Wenn Sie Änderungen vorgenommen haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren 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 Überprüfung anzufordern, melden Sie sich bei der AWS Konsole an und navigieren 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.

F8. 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.

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). Die Ursache muss von Ihnen selbst untersucht werden.

F10. 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](#) (p. 400).

F11. 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.

F12. Was passiert, wenn ich meine Korrekturen erst kurz vor Ende des Überprüfungszeitraums durchführe?

Melden Sie sich bei der AWS-Konsole an und navigieren 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.

F13. Kann ich über den zuständigen AWS-Mitarbeiter oder im Rahmen des Premium Supports Unterstützung bekommen?

Wenn Sie bereits mit einem AWS Kundenbetreuer zusammenarbeiten, wenden wir uns automatisch an diesen Mitarbeiter, wenn für Ihr Konto eine Prüfung festgelegt 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 [Nutzungsbedingungen AWS Dienstleistungen](#). 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 Adresse, die mit Ihrem AWS Konto verknüpft ist, finden Sie unter [Verwalten eines AWS-Kontos](#) im AWS Billing and Cost Management Benutzerhandbuch.

Sie können Amazon CloudWatch zum Erstellen von Alarmen nutzen, die Sie informieren, wenn Ihre Unzustellbarkeits- 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 CloudWatch finden Sie unter [Erstellen von Zuverlässigkeitsüberwachungsalarman mit CloudWatch](#) (p. 415).

Sie können auch das [Zustellbarkeits-Dashboard](#) (p. 400) verwenden, um den aktuellen Status Ihres Kontos zu bestimmen. Beispiel: Wenn die Fähigkeit Ihres Kontos zum Senden von E-Mails derzeit unterbrochen ist, zeigt der Abschnitt Account status (Kontostatus) des Zustellbarkeits-Dashboards den Status SENDING PAUSE (SENDEUNTERBRECHUNG) an. Wenn Ihr Konto E-Mails normal senden kann, zeigt es den Status HEALTHY (STABIL) an.

Abschließend können Sie die AWS Personal Health Dashboard (PHD) bei <https://phd.aws.amazon.com/> überprüfen Sie, ob die Fähigkeit Ihres Kontos, E-Mails zu versenden, derzeit unterbrochen ist. Wenn wir die Fähigkeit, E-Mails zu senden, vorübergehend unterbrechen, fügen wir automatisch ein SES sending paused (SES-Senden unterbrochen)-Ereignis dem Abschnitt Event log (Ereignisprotokoll) der PHD hinzu. Das SES sending paused (SES-Senden unterbrochen)-Ereignis 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 E-Mail-Adresse gesendet haben, die mit Ihrem AWS Konto verknüpft ist, wenn das Sendeunterbrechungs-Ereignis aufgetreten ist.

Sie können CloudWatch zum Erstellen von Alarmen nutzen, die Sie benachrichtigen, wenn neue Ereignisse in Ihrem Personal Health Dashboard angezeigt werden. Weitere Informationen finden Sie unter [Überwachung AWS Health Ereignisse mit CloudWatch Ereignissen](#) im AWS Health Benutzerhandbuch.

F4. Die Fähigkeit meines Kontos, E-Mails zu versenden, wurde unterbrochen. Hat dies Auswirkungen darauf, wie Sie andere AWS Dienste verwenden können?

Sie können weiterhin andere AWS Dienste verwenden, während die Fähigkeit Ihres Kontos zum Versenden von E-Mails unterbrochen ist. Wenn Sie jedoch eine Erhöhung des Servicekontingents für einen anderen AWS S-Service anfordern, der ausgehende Kommunikation sendet (z. B. Amazon SNS), lehnen wir diesen Antrag 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.
- Wenn Sie Änderungen vorgenommen haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren 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 Überprüfung anzufordern, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. Antworten Sie auf den Fall, den wir in Ihrem Namen eröffnet haben.

Machen Sie in Ihrer 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](#) (p. 400).

F11. Kann ich über den zuständigen AWS-Mitarbeiter oder im Rahmen des Premium Supports Unterstützung bekommen?

Wenn Sie bereits mit einem AWS Kundenbetreuer zusammenarbeiten, wenden wir uns automatisch an diesen Mitarbeiter, wenn für Ihr Konto die Fähigkeit zum Senden von E-Mails unterbrochen 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.

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. Wenn Sie Änderungen vorgenommen haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren 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 unter [F11. Was kann ich tun, um die Zahl unzustellbarer Nachrichten zu minimieren?](#) (p. 537) aufgeführten Empfehlungen Sie befolgen

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 betrachten wir ein repräsentatives Volumen 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 mithilfe der Informationen aus der Amazon SES Konsole oder der GetSendStatistics-API meine eigene Unzustellbarkeitsquote berechnen?

Nein. Die Unzustellbarkeitsquote wird anhand der repräsentativen Menge berechnet (siehe [F5. Über welche Zeitspanne hinweg wird meine Unzustellbarkeitsquote berechnet? \(p. 535\)](#)). Je nach Senderate kann Ihre Unzustellbarkeitsquote weiter zurückreichen, als Daten von der Amazon SES-Konsole oder der Amazon SES Konsole.`GetSendStatistics` abrufen kann. 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?

Überprüfen Sie die Unzustellbarkeitsbenachrichtigungen, die Amazon SES Ihnen sendet. Die E-Mail-Adresse, an die Amazon SES die Benachrichtigungen weiterleitet, hängt davon ab, wie Sie die ursprünglichen Nachrichten gesendet haben, wie unter beschrieben. [Per E-Mail gesendete Amazon SES S-Benachrichtigungen \(p. 289\)](#). Sie können auch Unzustellbarkeitsbenachrichtigungen über Amazon Simple Notification Service (Amazon SNS) einrichten, wie unter beschrieben. [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen \(p. 288\)](#). 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? \(p. 537\)](#).

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 [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen \(p. 288\)](#).

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 Sendekontingent zu überschreiten, erhalten Sie bei dem Versuch, eine E-Mail zu versenden, eine Fehlermeldung von der Amazon 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?](#) (p. 536)). 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 Amazon SES für Systembenachrichtigungen verwenden, stellen Sie sicher, dass Sie die Benachrichtigungen an echte E-Mail-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 E-Mail-Adressen senden, die E-Mails empfangen können, oder dass Sie den Amazon SES Postfachsimulator verwenden. Weitere Informationen finden Sie unter [Testen der E-Mail-Versendung in Amazon SES](#) (p. 198).

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 zum Melden von Spam geklickt, sich bei ihrem E-Mail-Anbieter beschwert, Amazon SES direkt oder auf andere Weise benachrichtigt. Dieses Thema enthält allgemeine Informationen zu Beschwerden. Wenn Ihre Benachrichtigung spezielle Informationen über die Quelle der Beschwerden enthält, lesen Sie auch die relevanten Themen: - [Beschwerden durch Feedback-Schleifen durch Amazon SES](#) (p. 538), [Amazon SES direkt von](#)

[Empfängern — Häufig gestellte Fragen \(p. 540\)](#) oder [Amazon SES durch E-Mail-Anbieter — Häufig gestellte Fragen \(p. 541\)](#).

F2. Warum interessieren Sie meine Beschwerden?

Hohe Beschwerdequoten dienen Organisationen wie E-Mail-Diensteanbietern 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. Wenn Sie Änderungen vorgenommen haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren 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, über die Amazon SES Sie informieren kann, überwachen, wobei es sich um Beschwerden handelt, die Amazon SES durch Feedback-Schleifen erhält (siehe [Beschwerden durch Feedback-Schleifen durch Amazon SES \(p. 538\)](#)) enthalten. 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.

-Beschwerden durch Feedback-Schleifen durch Amazon SES

In diesem Thema erhalten Sie Informationen zu Beschwerden, die Amazon SES von E-Mail-Anbietern durch Feedback-Schleifen erhält. Allgemeine Informationen, die für alle Arten von Beschwerden gelten, finden Sie unter [Beschwerden – Häufig gestellte Fragen \(p. 537\)](#).

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 Amazon SES eine Feedbackschleife (FBL) beim E-Mail-Anbieter eingerichtet hat, wird die Beschwerde zurück an Amazon SES gesendet.

F2. Sind diese Beschwerden in der Beschwerdequotenstatistik enthalten, die in der Amazon SES Konsole angezeigt und von der GetSendStatistics cs-API zurückgegeben wird?

Ja. Die Statistik zur Beschwerdequote enthält jedoch keine Beschwerden von E-Mail-Anbietern, die kein Feedback an Amazon SES senden. 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 [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen](#) (p. 288).

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 [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen](#) (p. 288).

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 beschwerten, beheben Sie nicht das zugrunde liegende Problem.

F5. Legen Sie die Beschwerdequoten von Amazon SES offen, die dazu führen könnten, dass eine Prüfung für mein Konto festgelegt oder die Fähigkeit meines Kontos zum Versenden von E-Mails 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 betrachten wir einrepräsentatives

Volumen 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. Sie wird berechnet als Prozentsatz von Beschwerden auf E-Mails, die an Domänen gesendet wurden, die Beschwerde-Feedback an Amazon SES senden.

F7. Kann ich mithilfe der Metriken aus der Amazon SES Konsole oder der `GetSendStatistics` cs-API meine eigene Beschwerdequote 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? \(p. 539\)](#)). Je nach Senderate kann Ihre Beschwerdequote weiter zurückreichen, als Daten von der Amazon SES-Konsole oder der Amazon SES Konsole.`GetSendStatistics`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 Beschwerdequote wird berechnet als Prozentsatz von Beschwerden auf E-Mails, die an Domänen gesendet wurden, die Beschwerde-Feedback an Amazon SES senden.

F8. Wie kann ich herausfinden, von welchen E-Mail-Adressen Beschwerden kamen?

Überprüfen Sie die Beschwerdebenachrichtigung, die Amazon SES Ihnen per E-Mail oder über Amazon SNS sendet (siehe [Überwachen des Amazon SES E-Mail-Versands mithilfe von Benachrichtigungen \(p. 288\)](#)) enthalten. Unterschiedliche E-Mail-Anbieter stellen jedoch Informationen in unterschiedlichem Umfang bereit und einige Anbieter machen die E-Mail-Adresse des Empfängers unkenntlich, bevor sie die Beschwerdebenachrichtigung an Amazon SES übermitteln. Damit Sie in Zukunft die E-Mail-Adresse des Empfängers finden können, empfiehlt sich eine Speicherung Ihrer eigenen Zuordnung zwischen einem Bezeichner und der Amazon SES Mitteilungs-ID, die Amazon SES zurücksendet, wenn er die E-Mail akzeptiert. Beachten Sie, dass Amazon SES keine benutzerdefinierte Mitteilungs-IDs speichert, die Sie hinzufügen.

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? \(p. 540\)](#).

Amazon SES direkt von Empfängern — Häufig gestellte Fragen

In diesem Thema erhalten Sie Informationen zu Beschwerden, die Amazon SES direkt von Empfängern erhält. Allgemeine Informationen, die für alle Arten von Beschwerden gelten, finden Sie unter [Beschwerden – Häufig gestellte Fragen \(p. 537\)](#).

F1. Wie wird diese Art Beschwerde gemeldet?

Mehrere Empfänger haben Amazon SES direkt per E-Mail oder auf anderem Wege bezüglich Ihrer E-Mails kontaktiert.

F2. Sind diese Beschwerden in der Beschwerdequotenstatistik enthalten, die in der Amazon SES Konsole angezeigt und von der GetSendStatistics cs-API zurückgegeben wird?

Nein. Die Beschwerdequotenstatistik, die Sie mithilfe der Amazon SES Konsole oder der `GetSendStatistics` API enthält nur Beschwerden, die Amazon SES durch Feedback-Schleifen erhält. Weitere Informationen zu diesen Arten von Beschwerden finden Sie unter [Beschwerden durch Feedback-Schleifen durch Amazon SES \(p. 538\)](#).

F3. Warum wurde ich nicht durch Feedback-Benachrichtigungen per E-Mail oder über Amazon SNS über diese Beschwerden informiert?

E-Mail-Feedback-Weiterleitung und Amazon SNS Benachrichtigungen enthalten nur Beschwerden, die Amazon SES durch Feedback-Schleifen erhält. Sie erhalten keine Benachrichtigungen über Beschwerden, die Empfänger direkt bei Amazon SES einreichen.

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 beschwerten.

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. Wenn Sie Änderungen vorgenommen haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren 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.

Amazon SES durch E-Mail-Anbieter — Häufig gestellte Fragen

In diesem Thema erhalten Sie Informationen zu Beschwerden, die Amazon SES von E-Mail-Anbietern erhält (die auch E-Mail-Dienstanbieter) enthalten. Allgemeine Informationen, die für alle Arten von Beschwerden gelten, finden Sie unter [Beschwerden – Häufig gestellte Fragen \(p. 537\)](#).

F1. Wie wird diese Art Beschwerde gemeldet?

Ein E-Mail-Anbieter meldete Amazon SES, dass eine beträchtliche Anzahl seiner Kunden Ihre E-Mails als Spam gekennzeichnet haben. Die Meldung wurde Amazon SES auf anderem Wege als über die unter beschriebenen Feedback-Schleifen bereitgestellt. [Beschwerden durch Feedback-Schleifen durch Amazon SES \(p. 538\)](#).

F2. Sind diese Beschwerden in der Beschwerdequotenstatistik enthalten, die in der Amazon SES Konsole angezeigt und von der `GetSendStatistics` cs-API zurückgegeben wird?

Nein. Die Beschwerdequotenstatistik, die Sie mithilfe der Amazon SES Konsole oder der `GetSendStatistics` API enthält nur Beschwerden, die Amazon SES durch Feedback-Schleifen erhält.

F3. Warum wurde ich nicht durch Feedback-Benachrichtigungen per E-Mail oder über Amazon SNS über diese Beschwerden informiert?

E-Mail-Feedback-Weiterleitung und Amazon SNS Benachrichtigungen enthalten nur Beschwerden, die Amazon SES durch 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. Wenn Sie Änderungen vorgenommen haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und navigieren 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 Domännennamen auf). Häufig, aber nicht immer, gelangen Spamtraps in die Welt, indem sie auf verschiedene Arten und Weisen im Internet platziert werden.

F3. Wie erkennt Amazon SES, dass ich an Spamfallen sende?

Bestimmte Organisationen, die Spamfallen betreiben, senden Amazon SES S-Benachrichtigungen, wenn ihre Spamfallen von Amazon SES-Absendern erreicht werden.

F4. Wie verwendet Amazon SES Berichte über Spamfallen?

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 bei der AWS Konsole an und navigieren 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 Amazon SES Prüfer hat ein gravierendes Problem mit Ihrem Senden von E-Mails entdeckt. Typische Probleme sind unter anderem folgende:

- Ihre Sendevorgänge verstoßen gegen die [AWS Acceptable Use Policy](#) (AUP).
- Ihre E-Mails scheinen unerwünscht zu sein.
- Die Inhalte stehen mit einem Anwendungsfall in Verbindung, den Amazon 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 Amazon SES, um sich über von Ihrem -Konto gesendete E-Mails zu beschweren.
- 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, die besagt, dass wir eine dieser Maßnahmen aufgrund eines Problems mit unerwünschten E-Mails ergreifen, melden Sie sich bei der AWS Konsole an und navigieren Sie zum Support Center. 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 den [Richtlinien für die AWS-Nutzung](#)?
- 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. Wenn Sie Änderungen vorgenommen haben, die das Problem Ihrer Ansicht nach beheben, melden Sie sich bei der AWS Konsole an und

navigieren 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 zum Support Center navigieren. Beantwortet auf den Fall, den wir in Ihrem Namen geöffnet haben, und fordert ein Beispiel der E-Mail an, die das Problem verursacht hat.

DNS-Blackhole-Liste (DNSBL) — Häufig gestellte Fragen

Domänenname Systembasierte Blackhole-Listen(DNSBLs) — manchmal auch alsEchtzeit-Sperrlisten(RBL),Listen verweigerung,Blocklisten, oderSperrlisten— sollen E-Mail-Anbieter über IP-Adressen informieren, die im Verdacht stehen, unerwünschte E-Mails zu senden.

Unterschiedliche DNSBLs haben unterschiedliche Auswirkungen auf die E-Mail-Zustellbarkeit. In diesem Thema wird beschrieben, wie sich DNSBLs auf die Bereitstellung von E-Mails auswirken können, die Sie mit Amazon SES senden, sowie unsere Richtlinien zum Entfernen unserer Amazon SES-IP-Adressen von DNSBL.

Note

In diesem Thema geht es um DNSBLs, die E-Mail-Dienstanbieter verwenden, um eingehende Nachrichten zu blockieren. Weitere Informationen darüber, wie Amazon SES ausgehende E-Mails blockiert, die an Empfänger gesendet wurden, deren E-Mail-Adressen zuvor Unzustellbarkeitsnachrichten generiert haben, finden Sie unter[Verwenden der globalen Unterdrückungsliste von Amazon SES \(p. 210\)](#)aus.

F1. Wie wirken sich DNSBLs auf die E-Mail-Zustellung aus?

Unterschiedliche DNSBLs haben unterschiedliche Auswirkungen auf die erfolgreiche Zustellung einer Nachricht. Große E-Mail-Anbieter — einschließlich Gmail, Hotmail, AOL und Yahoo — scheinen eine sehr kleine Anzahl von hoch angesehenen DNSBL zu erkennen, wie z. B. die Angebote von Spamhaus. Unserer Erfahrung nach haben andere DNSBLs normalerweise geringe Auswirkungen, obwohl einige E-Mail-Systeme für bestimmte DNSBLs eine höhere Priorität festlegen als für andere.

Schließlich verfügen viele E-Mail-Anbieter oft über eigene interne Ablehnungslisten. 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 gelangen IP-Adressen auf DNSBLs?

Es gibt verschiedene Möglichkeiten, die dazu führen, dass eine IP-Adresse auf einer DNSBL landet. IP-Adressen können DNSBLs hinzugefügt werden, wenn sie E-Mails an eine Pseudo-E-Mail-Adresse für Spamaus. 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 DNSBLs erlauben einzelnen Benutzern auch, IP-Adressen zu übermitteln. Einige DNSBLs erlauben Benutzern sogar, ganze IP-Adressbereiche zu übermitteln. Andere DNSBLs werden durch Beiträge von E-Mail-Administratoren gepflegt und können IP-Adressen enthalten, von denen Administratoren glauben, dass sie ihre eigenen Systeme missbrauchen.

F3. Wie kann Amazon SES verhindern, dass seine IP-Adressen auf DNSBLs erscheinen?

Unsere Systeme suchen nach Anzeichen eines Missbrauchs. Wenn wir Sendemuster oder andere Merkmale erkennen, die dazu führen, dass eine IP-Adresse zu einer DNSBL hinzugefügt wird, senden wir eine Benachrichtigung an den Absender. 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. Durch solche Maßnahmen zum Durchsetzen unserer Senderrichtlinien können wir das Risiko verringern, dass unsere IP-Adressen auf DNSBL landen.

F4. Kann Amazon SES seine IP-Adressen aus einer DNSBL entfernen lassen?

Wir überwachen aktiv solche DNSBLs, die Auswirkungen auf die Zustellung innerhalb des gesamten Amazon SES S--Service haben können oder auf die Fähigkeit zum Versenden von E-Mails an Empfänger, die großen E-Mail-Anbieter, wie z. B. Gmail, Yahoo, AOL und Hotmail, nutzen. Die von Spamhaus angebotenen DNSBL gehören zu dieser 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 aus der DNSBL entfernen zu lassen.

Wir überwachen keine DNSBLs, die sich mit geringer Wahrscheinlichkeit auf die Zustellung innerhalb des gesamten Amazon SES S--Service auswirken oder deren Auswirkung auf die Zustellung zu großen E-Mail-Anbietern nicht messbar ist. Die von SORBS und UCEPROTECT angebotenen DNSBL gehören zu dieser Kategorie. Aufgrund der spezifischen Auflistungs- und Löschverfahren der Anbieter, die diese Listen betreiben, können wir unsere IP-Adressen nicht aus diesen Listen entfernen lassen.

F5. Ein E-Mail-Anbieter lehnt meine E-Mail ab, da die IP-Adresse von einer DNSBL mit Ausnahme von Spamhaus aufgeführt wird. Was sollte ich tun?

Stellen Sie zunächst sicher, dass die Nachricht wirklich aufgrund einer DNSBL blockiert wurde. Wenn Ihre E-Mail abgelehnt wurde, weil die IP-Adresse einer DNSBL hinzugefügt wurde, erhalten Sie in der Regel eine Unzustellbarkeitsbenachrichtigung. Diese enthält den Namen des DNSBL-Betreibers, wie in dem folgenden Beispiel:

```
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 Domäne, die Sie kontaktieren möchten, ihre Postmaster-Support-Richtlinien nicht veröffentlicht, können Sie möglicherweise den Postmaster kontaktieren, indem Sie eine E-Mail `anpostmaster@example.com` wobei `example.com` Die betreffende Domäne ist. 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, dass 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 \(p. 188\)](#) 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. Durch gutes Sendeverhalten können Sie dazu beitragen, dass Ihre Adressen nicht auf DNSBLs landen.

F6. E-Mails, die ich an Gmail, Yahoo, Hotmail oder einen anderen wichtigen Anbieter sende, werden an den Spam-Ordner gesendet. Passiert das, weil sich meine IP-Adresse auf einer DNSBL befindet?

Wahrscheinlich nicht. Wenn eine IP-Adresse von einer DNSBL mit erheblichen Auswirkungen aufgeführt wird, wie z. B. einer der DNSBL von Spamhaus, werden große E-Mail-Anbieter E-Mail-Nachrichten von dieser IP-Adresse vollständig ablehnen, 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. Das Mieten oder Kaufen von Listen ist ein Verstoß gegen die [AccAWS table Use Policy \(AUP\)](#) und ist auf Amazon SES nicht 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 \(p. 141\)](#) und [DKIM \(p. 142\)](#).

- 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.

Häufig gestellte Fragen zu -E-Mail-Sendemetriken

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 häufig gestellte Fragen zu folgenden Themen in Zusammenhang mit E-Mail-Sendemetriken:

- [Allgemeine Fragen](#) (p. 549)
- [Öffnungsnachverfolgung](#) (p. 550)
- [Klicknachverfolgung](#) (p. 551)

Allgemeine Fragen

F1. Wie lange sammelt Amazon SES weitere 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. Wenn ein Empfänger mehrmals auf denselben Link klickt, zählt Amazon SES jeden Klick als einmaliges Klickereignis.

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 Öffnungs- und Klickmetriken für Amazon SES mithilfe der CloudWatch ch-API abrufen. Sie können beispielsweise die verwendenAWS CLISie können Klickmetriken über die CloudWatch ch-API abrufen, indem Sie den folgenden Befehl eingeben:

```
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?

Wir haben unten in jede E-Mail, die über Amazon SES gesendet wurde, ein transparentes GIF-Bild mit 1 x 1 Pixel eingefügt. Jede E-Mail enthält einen eindeutigen Verweis auf diese Bilddatei. Wenn das Bild geöffnet wird, kann Amazon SES genau feststellen, welche Nachricht von wem geöffnet wurde.

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.

Eine detaillierte Erläuterung dieses Vorgangs finden Sie unter [the section called “Überwachen des Versands mithilfe der Ereignisveröffentlichung” \(p. 313\)](#).

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 auf einen Link klicken, 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 einen Link zur AWS-Homepage erstellen, sieht ein normaler Anker-Link in etwa 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 es sich bei `ses:no-track` um 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. Weitere Informationen finden Sie unter [Verwalten von Veranstaltungszielen in Amazon SES](#) (p. 277).

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 ordnungsgemäß kodierte URLs enthalten. Insbesondere müssen URLs in Ihren Links den Standard [RFC 3986](#) erfüllen. 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 falscher Kodierung treten in der Regel bei URLs mit Abfragezeichenfolgen auf. Wenn beispielsweise die URL eines Links in Ihrer E-Mail ein nicht-kodiertes Leerzeichen in der Abfragezeichenfolge enthält (wie etwa das Leerzeichen zwischen "John" und "Doe", im folgenden Beispiel: `http://www.example.com/path/to/page?name=John Hans Muster`), wird Amazon SES diesen Link nicht verfolgen. Wenn jedoch die URL stattdessen ein kodiertes Leerzeichen enthält (z. B. „%20“ im folgenden Beispiel: `http://www.example.com/path/to/page?name=John%20Doe`), verfolgt Amazon SES es wie erwartet.

Amazon SES Ressourcen

Die folgende Tabelle enthält Ressourcen, die möglicherweise bei der Arbeit mit Amazon Simple Email Service (Amazon SES) hilfreich sind.

Ressource	Beschreibung
Amazon Simple Email Service API-Referenz	Die Amazon SES API-Referenz. Enthält eine umfassende Beschreibung der API-Aktionen, -Parameter und -Datentypen sowie eine Liste von Fehlern, die der Service zurückgibt.
Amazon SES – Preise	Die Preisübersicht für Amazon SES.
Erschließen von SES-Sending Limits	Das Support-Center-Formular, um eine Erhöhung Ihrer Sendekontingente zu beantragen und die Sandbox zu verlassen.
Amazon SES Forum	Ein Forum, in dem Amazon SES Benutzer Fragen stellen und verschiedene Amazon SES-Themen diskutieren können.
AWS Blog zu Messaging und Targeting	Das Blog mit Blog-Beiträgen und Ankündigungen des Amazon SES -Teams.
AWS-Entwickler-Tools	Links zu Entwicklertools und -Ressourcen mit Dokumentationen, Codebeispielen, Versionshinweisen und sonstigen Informationen für die Entwicklung innovativer Anwendungen mit AWS.
AWS Support-Center	Die Zentrale zum Anlegen und Verwalten Ihrer AWS Support-Fälle. Bietet außerdem Links zu hilfreichen Ressourcen wie z. B. Foren, technischen Fragen und Antworten, Übersicht zum Servicestatus und AWS Trusted Advisor.
Kontakt	Eine zentrale Anlaufstelle bei Fragen zu AWS-Abrechnungen, Konten, Vorfällen, Missbrauch und anderen Problemen.
AWS-Glossar	Das AWS Glossar. Enthält Definitionen allgemein verwendeter Begriffe in Amazon SES und anderen AWS -Services.
Nutzungsbedingungen	AccAWS table Use Policy. Beschreibt E-Mail-Missbrauch und andere verbotene Nutzungen der von Amazon Web Services, Inc. angebotenen Webservices.
email-abuse@amazon.com	Eine E-Mail-Adresse zum Melden von schädlichen oder unerwünschten E-Mails aus Amazon SES. Wenn Sie diese Adresse kontaktieren, geben Sie bitte die folgenden Informationen an: • Die vollständigen Header der E-Mail-Nachricht. Weitere Informationen zum Abrufen von E-Mail-Headern finden Sie unter https://support.google.com/mail/answer/22454?hl=en. • Die Art des Missbrauchs. Beispielsweise unerwünschte E-Mails ohne Möglichkeit zur Abmeldung.

-Entwicklerhandbuch — Anhang

Dieser Anhang enthält ergänzende Informationen zum Versenden von E-Mails über Amazon Simple Email Service (Amazon SES).

- Die Anforderungen an das Header-Feld für E-Mails, die Sie über Amazon SES versenden, finden Sie unter [Header-Felder \(p. 554\)](#) aus.
- Eine Liste der Anlagentypen, die Amazon SES nicht akzeptiert, finden Sie unter [Nicht-unterstützte Anhangtypen \(p. 556\)](#) aus.

Header-Felder

Amazon SES kann alle E-Mail-Header akzeptieren, die das in [RFC 822](#) aus.

Die folgenden Felder können nicht mehr als einmal im Header-Abschnitt einer Nachricht angezeigt werden:

- Accept-Language
- acceptLanguage

Note

Dieses Feld ist nicht standardmäßig. Sie sollten, wenn möglich, stattdessen den Accept-Language-Header verwenden.

- Archived-At
- Auto-Submitted
- Bounces-to
- Kommentare
- Content-Alternative
- Content-Base
- Content-Class
- Content-Description
- Content-Disposition
- Content-Duration
- Content-ID
- Content-Language
- Content-Length
- Content-Location
- Inhalt-MD5
- Content-Transfer-Encoding
- Content-Type
- Datum

Note

Wenn Sie einen Date-Header angeben, überschreibt ihn von Amazon SES mit einem Zeitstempel, der dem Datum und der Uhrzeit in der UTC-Zeitzone entspricht, als Amazon SES die Nachricht akzeptiert hat.

- Delivered-To

- Disposition-Notification-Options
- Disposition-Notification-To
- DKIM-Signature
- DomainKey-Signature
- Errors-To
- Aus
- Importance
- In-Reply-To
- Keywords
- List-Archive
- List-Help
- List-Id
- List-Owner
- List-Post
- List-Subscribe
- List-Unsubscribe
- Message-Context
- Message-ID

Note

Wenn Sie einen Message-ID-Header angeben überschreibt Amazon SES den Header mit dem eigenen Wert.

- MIME-Version
- Organisation
- Original-From
- Original-Message-ID
- Original-Recipient
- Original-Subject
- Precedence
- Priorität
- Referenzen
- Reply-To
- Return-Path

Note

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.

- Return-Receipt-To
- Sender
- Solicitation
- Sensitivity
- Betreff
- Thread-Index
- Thread-Topic
- User-Agent
- VBR-Info

Nicht-unterstützte Anhangtypen

Sie können Nachrichten mit Anhängen über Amazon SES versenden, indem Sie den MIME-Standard (Multipurpose Internet Mail Extensions) verwenden. Amazon SES akzeptiert alle Dateianhängentypen außer für Anhängen mit den Dateierweiterungen in der folgenden Liste auf.

Note

Einige ISPs haben weitere Beschränkungen (z. B. Beschränkungen bezüglich archivierter Anhänge). Daher empfehlen wir Ihnen, Ihren E-Mail-Versand über die wichtigsten ISPs zu testen, bevor Sie Ihre Produktions-E-Mails versenden.

.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

Dokumentverlauf für Amazon SES Entwicklerhandbuch

In der folgenden Tabelle sind die wichtigen Änderungen am Amazon Simple Email Service (Amazon SES) - Entwicklerhandbuch.

Änderung	Beschreibung	Datum geändert
Neue Funktion	Sie können jetzt eine Standardkonfigurationssatz (p. 274) , die beim Senden von E-Mails über jede Ihrer verifizierten Identitäten verwendet werden soll.	27. Januar 2021
Neue Funktion	Sie können jetzt Benachrichtigungen (p. 313) erhalten, wenn ein Ereignis eintritt, das vorübergehend zu einer verzögerten Zustellung einer E-Mail führt.	19. Juni 2020
Neue Funktion	Amazon SES ist jetzt in der Region verfügbar AWS GovCloud (US) (p. 494) .	30. April 2020
Neue Funktion	Sie können jetzt mit fortfahren Erstellen von Amazon SES Endpunkten in Amazon Virtual Private Cloud (p. 89) (Amazon VPC).	29. April 2020
Neue Funktion	Amazon SES ist jetzt in der Region verfügbar drei weitere AWS Regionen (p. 494) : Kanada (Zentral), Europa (London) und Südamerika (São Paulo).	01. April 2020
Neue Funktion	Sie können jetzt Ihre eigenen IP-Bereiche verwenden, um E-Mails zu senden. Weitere Informationen finden Sie unter Verwenden Ihrer eigenen IP-Adressen zum Senden von E-Mails mit Amazon SES verwenden (p. 197) .	23. Dezember 2019
Neue Funktion	Sie können jetzt Ihr eigenes Schlüsselpaar aus öffentlichem und privatem Schlüssel verwenden, um den DKIM-Authentifizierungsprozess für eine Domäne abzuschließen. Weitere Informationen finden Sie unter Bereitstellen Ihres eigenen DKIM-Authentifizierungs-Tokens in Amazon SES (p. 150) .	13. Dezember 2019
Neue Funktion	Sie können nun eine Unterdrückungsliste auf Kontoebene (p. 201) verwenden, um automatisch zu verhindern, dass Nachrichten an E-Mail-Adressen gesendet werden, die zuvor zu einer Unzustellbarkeit oder einer Beschwerde geführt haben.	25. November 2019
Neue Funktion	Wenn Ihr Konto in Ordnung ist und Sie sich den Sendekontingenten für Ihr Konto nähern, erhöht Amazon SES automatisch Ihre Kontingente. Weitere Informationen finden Sie unter Erhöhen Ihrer Amazon SES Versandkontingente (p. 159) .	
Aktualisierung der Dokumentation	hinzugefügt Informationen zum Löschen personenbezogener Daten aus Amazon SES (p. 523) .	13. März 2018

Änderung	Beschreibung	Datum geändert
Open-Source-Code-Dokumentation	Die Amazon SES Dokumentation ist jetzt auf der Region verfügbar. GitHub . Sie können Probleme mitteilen oder Änderungen im GitHub-Repository anfordern bzw. Änderungen direkt vornehmen und eine Pull-Anforderung senden.	22. Februar 2018
Aktualisierung der Dokumentation	Es wurde ein Abschnitt mit Informationen über die Region hinzugefügt. Löschen personenbezogener Daten (p. 523) die in Amazon SES gespeichert sind.	28. Februar 2018
Aktualisierung der Dokumentation	Inhalte zur Überarbeitung Amazon SNS Ereignisveröffentlichungsfelddefinitionen (p. 349) , und fügte eine Rendering-Failure-Ereignis (p. 368) .	22. Januar 2018
Aktualisierung der Dokumentation	Der Zustellbarkeits-Dashboard-Anhang wurde so aktualisiert, dass Änderungen an den IAM- und Lambda-Konsolen berücksichtigt wurden. Note Wir haben diesen Anhang am 3. Mai 2019 entfernt, da er Komponenten verwendet hat, die nicht mehr unterstützt wurden.	18. Januar 2018
Aktualisierung der Dokumentation	Aktualisiert Inhalte zum Veröffentlichen von Ereignissen in CloudWatch (p. 316) , um blockierte Felder zu erwähnen.	15. Januar 2018
Aktualisierung der Dokumentation	Die Verfahren zum Versenden von E-Mail mithilfe von OpenSSL (p. 113) wurden aktualisiert, um sie leichter verständlich zu machen.	11. Januar 2018
Aktualisierung der Dokumentation	Ein Code-Beispiel für das Versenden von Raw-E-Mail mithilfe von AWS SDK for Ruby wurde hinzugefügt.	2. Januar 2018
Aktualisierung der Dokumentation	Ein Code-Beispiel für das Versenden von Raw-E-Mail mithilfe von AWS SDK for PHP wurde hinzugefügt.	29. Dezember 2017
Neue Funktion	Inhalten im Zusammenhang mit benutzerdefinierten Verifizierungs-E-Mails wurden hinzugefügt.	7. Dezember 2017
Neue Funktion	Inhalte im Zusammenhang mit dem Pausieren des E-Mail-Versands und dem Exportieren von Zuverlässigkeitsmetriken für Konfigurationssätze wurden hinzugefügt.	15. November 2017
Aktualisierung der Dokumentation	Ein Code-Beispiel für das Versenden von Raw-E-Mail mithilfe von AWS SDK for Java wurde hinzugefügt.	23. Oktober 2017
Aktualisierung der Dokumentation	Ein Code-Beispiel für das Versenden von Raw-E-Mail mithilfe von AWS SDK for Python (Boto) wurde hinzugefügt.	20. Oktober 2017
Neue Funktion	Inhalte im Zusammenhang mit E-Mail-Vorlagen und personalisierten E-Mail-Funktionen wurden hinzugefügt.	11. Oktober 2017

Änderung	Beschreibung	Datum geändert
Neue Funktion	Inhalte im Zusammenhang mit der Funktion für das Öffnen und Anklicken benutzerdefinierter Domänen wurden hinzugefügt.	18. September 2017
Neue Funktion	Inhalte im Zusammenhang mit dem Reputation Dashboard wurden hinzugefügt.	24. August 2017
Neue Funktion	Inhalte im Zusammenhang mit der Funktion für dedizierte IP-Pools wurden hinzugefügt.	17. August 2017
Neue Funktion	Inhalte im Zusammenhang mit der Nachverfolgungsfunktion für Öffnen und Klicken wurden hinzugefügt.	1. August 2017
Aktualisierung der Dokumentation	Index von Code-Beispielen wurde hinzugefügt.	26. Juni 2017
Aktualisierung der Dokumentation	Es wurde ein Anhang hinzugefügt, der das Erstellen eines Zustellbarkeits-Dashboards für Amazon SES veranschaulicht wurde. Note Wir haben diesen Anhang am 3. Mai 2019 entfernt, da er Komponenten verwendet hat, die nicht mehr unterstützt wurden.	22. Juni 2017
Aktualisierung der Dokumentation	Codebeispiele für das Senden von E-Mails wurden aktualisiert.	6. Juni 2017
Neue Funktion	Inhalte zu dedizierten IP-Adressen wurden hinzugefügt.	21. November 2016
Neue Funktion	Inhalte zur Ereignisveröffentlichung für das Senden von E-Mails wurden hinzugefügt.	2. November 2016
Service-Aktualisierung	Inhalte darüber, dass Benutzer nach dem Generieren ihrer DKIM-Datensätze nicht mehr explizit die Easy DKIM-Anmeldung aktivieren müssen, wurden hinzugefügt.	15. September 2016
Aktualisierung der Dokumentation	Tutorial für die ersten Schritte beim Empfangen von E-Mails wurde hinzugefügt.	12. Juli 2016
Neue Funktion	Inhalte zu erweiterten Benachrichtigungen wurden hinzugefügt.	14. Juni 2016
Neue Funktion	Inhalte zu benutzerdefinierten MAIL FROM-Domänen wurden hinzugefügt.	14. März 2016
Neue Funktion	Inhalte zu eingehenden E-Mails wurden hinzugefügt.	28. September 2015
Neue Funktion	Inhalte zur Sendeautorisierung wurden hinzugefügt.	8. Juli 2015
Neue Funktion	Inhalte zur AWS CloudTrail-Protokollierung wurden hinzugefügt.	7. Mai 2015
Service-Aktualisierung	Inhalte zur Konsolidierung der Formulare zur Erhöhung der Amazon SES Kontingente wurden hinzugefügt, der Begriff „production access“ wurde entfernt.	8. April 2015

Änderung	Beschreibung	Datum geändert
Service-Aktualisierung	Neue Anforderungen für TXT-Datensätze zur Domänenverifizierung wurden hinzugefügt.	25. Februar 2015
Aktualisierung der Dokumentation	Häufig gestellte Fragen zur Richtliniendurchsetzung wurden hinzugefügt.	15. Dezember 2014
Neue Funktion	Inhalte zu Zustellungsbenachrichtigungen wurden hinzugefügt.	23. Juni 2014
Neue Funktion	Inhalte zur Subdomänenunterstützung wurden hinzugefügt.	19. März 2014
Neue Funktion	Inhalte zur Erweiterung von Amazon SES in die Region USA West (Oregon) wurden hinzugefügt.	29. Januar 2014
Neue Funktion	Inhalte zur Erweiterung von Amazon SES auf die Region Europa (Irland) wurden hinzugefügt.	15. Januar 2014
Neue Funktion	Inhalte aufgrund der Änderungen bei der Validierung von Header-Feldern und MIME-Typen wurden hinzugefügt.	6. November 2013
Aktualisierung der Dokumentation	Inhalte zur Sender-ID wurden entfernt.	22. August 2013
Neue Funktion	Inhalte zur Überarbeitung der Amazon SES Konsole wurden hinzugefügt.	19. Juni 2013
Neue Funktion	Sie wurde in die globale Unterdrückungsliste umbenannt.	8. Mai 2013
Neue Funktion	Inhalte zum Entfernen von globalen Unterdrückungslisten wurden hinzugefügt.	4. März 2013
Aktualisierung der Dokumentation	MIME-Typen wurden hinzugefügt.	4. Februar 2013
Aktualisierung der Dokumentation	Ein Abschnitt mit ersten Schritten wurde hinzugefügt, der das eigenständige Handbuch "Erste Schritte" ersetzt. Das Inhaltsverzeichnis wurde neu strukturiert und die Sendmail-Integrationsanweisungen wurden aktualisiert.	January 21, 2013
Aktualisierung der Dokumentation	Abschnitte zur Fehlerbehebung im Hinblick auf das Erhöhen des Durchsatzes und SMTP-Probleme wurden hinzugefügt.	12. Dezember 2012
Aktualisierung der Dokumentation	Informationen zu Sendekontingenten wurden neu strukturiert.	9. November 2012
Neue Funktion	Inhalte zum Amazon SES Postfachsimulator wurden hinzugefügt.	3. Oktober 2012
Neue Funktion	Inhalte zur Verwendung einer DKIM-Signatur zum Signieren von E-Mails von einer verifizierten Identität wurden hinzugefügt.	17. Juli 2012

Änderung	Beschreibung	Datum geändert
Neue Funktion	Inhalte zum Empfangen von Unzustellbarkeits- und Beschwerdebenachrichtigungen über Amazon Simple Notification Service (Amazon SNS) wurden hinzugefügt.	26. Juni 2012
Neue Funktion	Inhalte zur Domänenverifizierung wurden hinzugefügt.	15. Mai 2012
Neue Funktion	Inhalte zu zusätzlichen Header- und Anhangtypen wurden hinzugefügt.	25. April 2012
Neue Funktion	Inhalte zur STARTTLS-Erweiterung für SMTP wurden hinzugefügt.	7. März 2012
Neue Funktion	Inhalte zu Variable Envelope Return Path (VERP) wurden hinzugefügt.	22. Februar 2012
Neue Funktion	Inhalte zur SMTP-Unterstützung wurden hinzugefügt.	13. Dezember 2011
Neue Funktion	Inhalte zur Unterstützung der AWS Management Console wurden hinzugefügt.	17. November 2011
Neue Funktion	Inhalte zur Unterstützung von Anhängen wurden hinzugefügt.	18. Juli 2011
Erstversion	Dies ist die erste Version des Amazon Simple Email Service — Entwicklerhandbuch.	25. Januar 2011

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.