aws

Benutzerhandbuch

Amazon WorkMail

Version 1.0

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon WorkMail: Benutzerhandbuch

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist Amazon WorkMail? ... 1
WorkMail Amazon-Systemanforderungen ... 1
WorkMail Amazon-Konzepte ... 2
Zugehörige AWS-Services ... 4
WorkMail Amazon-Preisgestaltung ... 5
Ressourcen ... 5
Voraussetzungen ... 6
Melden Sie sich an für ein AWS-Konto ... 6
Erstellen eines Benutzers mit Administratorzugriff ... 7
Erteilen Sie IAM-Benutzerberechtigungen für Amazon WorkMail ... 8
Sicherheit ... 9
Datenschutz ... 10
So WorkMail nutzt Amazon AWS KMS ... 11
Identity and Access Management ... 21
Zielgruppe ... 21
Authentifizierung mit Identitäten ... 22
Verwalten des Zugriffs mit Richtlinien ... 26
So WorkMail arbeitet Amazon mit IAM ... 29
Beispiele für identitätsbasierte Richtlinien ... 35
Fehlerbehebung ... 42
AWS verwaltete Richtlinien ... 44
AmazonWorkMailFullAccess ... 45
AmazonWorkMailReadOnlyAccess ... 45
AmazonWorkMailEventsServiceRolePolicy ... 45
Richtlinienaktualisierungen ... 46
Verwenden von serviceverknüpften Rollen ... 46
Servicebezogene Rollenberechtigungen für Amazon WorkMail ... 47
Eine serviceverknüpfte Rolle für Amazon erstellen WorkMail ... 48
Bearbeitung einer serviceverknüpften Rolle für Amazon WorkMail ... 48
Löschen einer serviceverknüpften Rolle für Amazon WorkMail ... 48
Unterstützte Regionen für Rollen im WorkMail Zusammenhang mit Amazon Services ... 49
Protokollierung und Überwachung ... 50
Überwachung mit CloudWatch Metriken ... 51
Überwachung der WorkMail E-Mail-Ereignisprotokolle von Amazon ... 55

Überwachung der WorkMail Amazon-Auditprotokolle 62
CloudWatch Insights mit Amazon verwenden WorkMail 69
Protokollierung Amazon WorkMail Amazon-API-Aufrufen mit AWS CloudTrail 73
Die Protokollierung von E-Mail-Ereignissen aktivieren 77
Audit-Protokollierung aktivieren 82
Compliance-Validierung 96
Ausfallsicherheit 97
Sicherheit der Infrastruktur 97
Erste Schritte 99
Erste Schritte mit Amazon WorkMail 99
Schritt 1: Melden Sie sich bei der WorkMail Amazon-Konsole an 100
Schritt 2: Richten Sie Ihre WorkMail Amazon-Website ein 100
Schritt 3: WorkMail Amazon-Benutzerzugriff einrichten 101
Weitere -Quellen 102
Zu Amazon migrieren WorkMail 102
Schritt 1: Benutzer in Amazon erstellen oder aktivieren WorkMail 102
Schritt 2: Zu Amazon migrieren WorkMail 102
Schritt 3: Schließen Sie die Migration zu Amazon ab WorkMail 103
Interoperabilität zwischen Amazon WorkMail und Microsoft Exchange 104
Voraussetzungen 104
Hinzufügen von Domänen und Aktivieren von Postfächern 105
Aktivieren der Interoperabilität 106
Dienstkonten in Microsoft Exchange und Amazon erstellen WorkMail 106
Beschränkungen im Interoperabilitätsmodus 107
Verfügbarkeitseinstellungen bei Amazon konfigurieren WorkMail 107
Konfigurieren Sie einen EWS-basierten Verfügbarkeitsanbieter 108
Konfiguration eines Anbieters für benutzerdefinierte Verfügbarkeit 109
Aufbau einer CAP-Lambda-Funktion 110
Konfigurieren der Verfügbarkeitseinstellungen in Microsoft Exchange 119
E-Mail-Routing zwischen Microsoft Exchange- und WorkMail Amazon-Benutzern aktivieren 120
Aktivieren der E-Mail-Weiterleitung für einen Benutzer 120
Konfiguration nach dem Einrichten 122
Mail-Client-Konfiguration 122
Deaktivierung des Interoperabilitätsmodus und Außerbetriebnahme Ihres Mailservers 123
Fehlerbehebung 124
WorkMail Amazon-Kontingente 125

WorkMail Amazon-Organisations- und Benutzerkontingente 126
WorkMail Organisation, die Quoten festlegt 128
Kontingente pro Benutzer 129
Nachrichtenkontingente 130
Arbeiten mit Organisationen 131
Erstellen einer Organisation 131
Erstellen einer Organisation 133
Die Details einer Organisation anzeigen 134
Ein WorkSpaces Verzeichnis integrieren 135
Organisationszustände und Beschreibungen 135
Löschen einer Organisation 136
Eine E-Mail-Adresse finden 137
Mit Organisationseinstellungen arbeiten 137
Postfachmigration aktivieren 138
Journaling aktivieren 138
Interoperabilität aktivieren 138
SMTP-Gateways aktivieren 138
E-Mail-Fluss verwalten 140
Durchsetzen von DMARC-Richtlinien für eingehende E-Mails 165
Markieren einer Organisation 166
Arbeiten mit Zugriffssteuerungsregeln 168
Erstellen von Zugriffssteuerungsregeln 169
Bearbeiten von Zugriffssteuerungsregeln 170
Testen von Zugriffssteuerungsregeln 171
Löschen von Zugriffssteuerungsregeln 171
Festlegen von Postfachaufbewahrungsrichtlinien 172
Arbeiten mit Domänen 174
Hinzufügen einer Domäne 174
Entfernen einer Domäne 179
Auswählen der Standarddomäne 179
Verifizieren von Domänen 180
Überprüfen von TXT-Datensätzen und MX-Datensätzen mit Ihrem DNS-Service 181
Fehlerbehebung bei der Domänenverifizierung 184
Aktivierung AutoDiscover zur Konfiguration von Endpunkten 186
AutoDiscover Phase 2: Fehlerbehebung 190
Bearbeiten von Domänenidentitätsrichtlinien 192

Benutzerdefinierte Amazon SES SES-Serviceprinzipalrichtlinie ... 193
Authentifizierung Ihrer E-Mails mit SPF ... 194
Konfiguration einer benutzerdefinierten MAIL FROM-Domäne ... 194
Working with users ... 196
Eine Benutzerliste anzeigen ... 196
Hinzufügen eines Benutzers ... 197
Aktivieren von Benutzern ... 198
Benutzer-Aliase verwalten ... 198
Deaktivieren von Benutzern ... 200
Editing user details ... 200
Das Benutzerkennwort wird zurückgesetzt ... 203
Fehlerbehebung bei WorkMail Amazon-Passwortrichtlinien ... 204
Working with notifications ... 205
Enabling signed or encrypted email ... 210
Arbeiten mit -Gruppen ... 211
Eine Liste von Gruppen anzeigen ... 211
Eine Gruppe hinzufügen ... 212
Gruppen aktivieren ... 213
Mitglieder zu einer Gruppe hinzufügen ... 213
Gruppendetails bearbeiten ... 214
Mitglieder aus einer Gruppe entfernen ... 215
Gruppenaliase verwalten ... 215
Gruppen deaktivieren ... 217
Löschen einer Gruppe ... 217
Arbeiten mit -Ressourcen ... 219
Eine Liste von Ressourcen anzeigen ... 219
Eine Ressource hinzufügen ... 220
Ressourcendetails bearbeiten ... 220
Ressourcen-Aliase verwalten ... 223
Eine Ressource aktivieren ... 224
Eine Ressource deaktivieren ... 225
Eine Ressource wird gelöscht ... 225
Arbeiten mit IAM Identity Center ... 227
IAM Identity Center in Amazon aktivieren WorkMail ... 229
Zuweisen von IAM Identity Center-Benutzern und -Gruppen zu Amazon-Anwendungen WorkMail ... 230

WorkMail Amazon-Benutzer mit IAM Identity Center-Benutzern verknüpfen 232
Authentifizierungsmodus 233
Konfiguration persönlicher Zugriffstoken 235
IAM Identity Center wird deaktiviert 236
Arbeiten mit mobilen Geräten 238
Bearbeiten der Mobilgeräte-Richtlinie Ihrer Organisation 238
Managing mobile devices 239
Remotely wiping mobile devices 239
Removing user devices from the devices list 241
Viewing mobile device details 241
Zugriffsregeln für mobile Geräte verwalten 242
So funktionieren die Zugriffsregeln für mobile Geräte 244
Verwenden von Zugriffsregeln für mobile Geräte 244
Überschreibungen für den Zugriff auf mobile Geräte verwalten 246
So funktionieren Überschreibungen für den Zugriff auf mobile Geräte 247
Überschreibungen verwalten 247
Integration mit Verwaltungslösungen für mobile Geräte 248
Überblick über die Verwaltungslösungen für mobile Geräte 249
Konfiguration einer WorkMail Organisation für die Integration mit einer MDM-Lösung eines Drittanbieters im Direktmodus 250
Arbeiten mit Postfachberechtigungen 253
Über Postfach- und Ordnerberechtigungen 254
Verwaltung der Postfachberechtigungen für Benutzer 255
Hinzufügen von Berechtigungen 255
Postfachberechtigungen für Benutzer bearbeiten 256
Verwaltung von Postfachberechtigungen für Gruppen 257
Programmatischer Zugriff auf Postfächer 259
Verwaltung von Identitätswechselrollen 259
Überblick über die Rollen beim Identitätswechsel 260
Sicherheitsüberlegungen 261
Rollen mit Identitätswechsel erstellen 261
Rollen mit Identitätswechsel bearbeiten 262
Testen von Rollen mit Identitätswechsel 264
Impersonationsrollen löschen 264
Verwenden von Rollen mit Identitätswechsel 265
Postfachinhalt exportieren 268

Voraussetzungen 268
Beispiele für IAM-Richtlinien und Rollenerstellung 269
Beispiel: Exportieren von Postfachinhalten 271
Überlegungen 272
Fehlerbehebung 190
Viewing email headers 273
E-Mail-Weiterleitung 273
E-Mail-Journaling mit Amazon verwenden WorkMail 275
Verwenden des E-Mail-Journals 275
Dokumentverlauf 277
..... cclxxxvii

Was ist Amazon WorkMail?

Amazon WorkMail ist ein sicherer, verwalteter E-Mail- und Kalenderservice für Unternehmen, der bestehende Desktop- und mobile E-Mail-Clients unterstützt. WorkMail Amazon-Benutzer können mit Microsoft Outlook, ihrem Browser oder ihren nativen iOS- und Android-E-Mail-Anwendungen auf ihre E-Mails, Kontakte und Kalender zugreifen. Sie können Amazon in Ihr WorkMail bestehendes Unternehmensverzeichnis integrieren und sowohl die Schlüssel zur Verschlüsselung Ihrer Daten als auch den Speicherort Ihrer Daten kontrollieren.

Eine Liste der unterstützten AWS-Regionen und Endpunkte finden Sie unter Regionen und Endpunkte von AWS.

Themen

- WorkMail Amazon-Systemanforderungen
- WorkMail Amazon-Konzepte
- Zugehörige AWS-Services
- WorkMail Amazon-Preisgestaltung
- WorkMail Amazon-Ressourcen

WorkMail Amazon-Systemanforderungen

Wenn Ihr WorkMail Amazon-Administrator Sie auffordert, sich bei Ihrem WorkMail Amazon-Konto anzumelden, können Sie sich mit dem WorkMail Amazon-Webclient anmelden.

Amazon funktioniert WorkMail auch mit allen gängigen Mobilgeräten und Betriebssystemen, die das ActiveSync Exchange-Protokoll unterstützen. Zu diesen Geräten zählen iPad, iPhone, Android- und Windows-Telefone. Benutzer von macOS können ihr WorkMail Amazon-Konto zu ihren Mail-, Kalender- und Kontakte-Apps hinzufügen.

Amazon WorkMail unterstützt die folgenden Betriebssystemversionen:

- Windows — Windows 7 SP1 oder höher
- macOS — macOS 10.12 (Sierra) oder höher
- Android — Andriod 5.0 oder höher
- iPhone — iOS 5 oder höher

- Windows Phone — Windows 8.1 oder höher
- Blackberry — Blackberry OS 10.3.3.3216

Wenn Sie über eine gültige Microsoft Outlook-Lizenz verfügen, können Sie WorkMail mit den folgenden Versionen von Microsoft Outlook auf Amazon zugreifen:

- Outlook 2013 oder höher
- Outlook 2013 Click-to-Run oder später
- Outlook für Mac 2016 oder höher

Sie können mit den folgenden Browserversionen auf den Amazon WorkMail Web Client zugreifen:

- Google Chrome — Version 22 oder höher
- Mozilla Firefox — Version 27 oder höher
- Safari — Version 7 oder höher
- Internet Explorer — Version 11
- Microsoft Edge

Sie können Amazon auch WorkMail mit Ihrem bevorzugten IMAP-Client verwenden.

WorkMail Amazon-Konzepte

Die Terminologie und Konzepte, die für Ihr Verständnis und Ihre Nutzung von Amazon von zentraler Bedeutung WorkMail sind, werden im Folgenden beschrieben.

Organisation

Ein Mandanten-Setup für Amazon WorkMail.

Alias

Ein global eindeutiger Name zur Identifizierung Ihrer Organisation. Der Alias wird für den Zugriff auf die WorkMail Amazon-Webanwendung (https://*alias*.awsapps.com/mail) verwendet.

Domain

Die Webadresse, die nach dem @ Symbol in einer E-Mail-Adresse steht. Sie können eine Domäne hinzufügen, die E-Mails empfängt und an Postfächer in Ihrem Unternehmen weiterleitet.

Test-Maildomäne

Während der Einrichtung wird automatisch eine Domain konfiguriert, die zum Testen von Amazon verwendet werden kann WorkMail. Die Test-Mail-Domain lautet *alias* .awsapps.com und wird als Standarddomain verwendet, wenn Sie Ihre eigene Domain nicht konfigurieren. Die Test-Maildomäne unterliegt unterschiedlichen Beschränkungen. Weitere Informationen finden Sie unter WorkMail Amazon-Kontingente.

Verzeichnis

Ein AWS Simple AD, AWS Managed AD oder AD Connector, der in erstellt wurde AWS Directory Service. Wenn Sie mit dem Amazon WorkMail Quick Setup eine Organisation erstellen, erstellen wir ein WorkMail Verzeichnis für Sie. Sie können ein WorkMail Verzeichnis nicht in anzeigen AWS Directory Service.

Benutzer

Ein Benutzer wurde im erstellt AWS Directory Service. Der Benutzer kann in einer USER - oder REMOTE_USER-Rolle erstellt werden. Wenn ein Benutzer mit einer USER-Rolle erstellt und aktiviert wird, erhält er sein eigenes Postfach, auf das er zugreifen kann. Wenn ein Benutzer deaktiviert ist, kann er nicht auf Amazon zugreifen WorkMail.

Benutzer, die mit einer REMOTE_USER-Rolle erstellt und aktiviert wurden, sind im Adressbuch aufgeführt, erhalten jedoch kein Postfach in Amazon. WorkMail Der REMOTE_USER kann das Postfach außerhalb von Amazon hosten lassen, wird WorkMail aber trotzdem wie jeder andere Benutzer mit Postfach im WorkMail Amazon-Adressbuch aufgeführt und kann im Kalender des jeweils anderen nach freien oder belegten Informationen suchen.

Gruppe

Eine Gruppe, die in verwendet wird. AWS Directory Service Eine Gruppe kann als Verteilerliste oder Sicherheitsgruppe in Amazon verwendet WorkMail werden. Gruppen haben keine eigenen Postfächer.

Ressource

Eine Ressource steht für einen Besprechungsraum oder eine Ausrüstungsressource, die von WorkMail Amazon-Benutzern gebucht werden kann.

Richtlinie für Mobilgeräte

Verschiedene Regeln für IT-Richtlinien, die die Sicherheitsmerkmale und das Verhalten eines mobilen Geräts steuern.

Zugehörige AWS-Services

Die folgenden Dienste werden zusammen mit Amazon genutzt WorkMail:

- AWS Directory Service—Sie können Amazon in ein WorkMail vorhandenes AWS Simple AD, AWS Managed AD oder AD Connector integrieren. Erstellen Sie ein Verzeichnis in AWS Directory Service und aktivieren Sie dann Amazon WorkMail für dieses Verzeichnis. Nachdem Sie diese Integration konfiguriert haben, können Sie WorkMail aus einer Liste von Benutzern in Ihrem vorhandenen Verzeichnis auswählen, welche Benutzer Sie für Amazon aktivieren möchten, und Benutzer können sich mit ihren vorhandenen Active Directory-Anmeldeinformationen anmelden. Weitere Informationen finden Sie im AWS Directory Service Administratorhandbuch.
- Amazon Simple Email Service — Amazon WorkMail verwendet Amazon SES, um alle ausgehenden E-Mails zu versenden. Die Test-Mail-Domain und Ihre Domains können in der Amazon SES-Konsole verwaltet werden. Für ausgehende E-Mails, die von Amazon gesendet werden, fallen keine Kosten an WorkMail. Weitere Informationen finden Sie im Amazon Simple Email Service Developer Guide.
- AWS Identity and Access Management— Sie AWS Management Console benötigen Ihren Benutzernamen und Ihr Passwort, damit jeder Dienst, den Sie verwenden, feststellen kann, ob Sie berechtigt sind, auf seine Ressourcen zuzugreifen. Wir empfehlen Ihnen, die Verwendung von AWS-Kontoanmeldedaten für den Zugriff zu vermeiden, AWS da AWS Kontoanmeldedaten in keiner Weise gesperrt oder eingeschränkt werden können. Stattdessen empfehlen wir, einen IAM-Benutzer zu erstellen und den Benutzer einer IAM-Gruppe mit Administratorberechtigungen hinzuzufügen. Anschließend können Sie mit den IAM-Benutzeranmeldedaten auf die Konsole zugreifen.

  Wenn Sie sich zwar bei AWS angemeldet, aber noch keinen eigenen IAM-Benutzer erstellt haben, können Sie dies mit der IAM-Konsole tun. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Individuelle IAM-Benutzer erstellen.
- AWS Key Management Service—Amazon WorkMail ist AWS KMS für die Verschlüsselung von Kundendaten integriert. Die Schlüsselverwaltung kann von der AWS KMS Konsole aus durchgeführt werden. Weitere Informationen finden Sie AWS Key Management Service im AWS Key Management Service Entwicklerhandbuch unter Was ist das?.

WorkMail Amazon-Preisgestaltung

Bei Amazon WorkMail fallen keine Vorabgebühren oder Verpflichtungen an. Sie zahlen nur für aktive Benutzerkonten. Weitere Informationen zu Preisen erhalten Sie unter Preise.

WorkMail Amazon-Ressourcen

Die folgenden verwandten Ressourcen bieten Ihnen nützliche Informationen für die Arbeit mit diesem Service.

- Kurse und Workshops — Links zu rollen- und Spezialkursen sowie zu Übungen zum Selbststudium, mit denen Sie Ihre AWS Fähigkeiten verbessern und praktische Erfahrungen sammeln können.
- AWS Developer Center — Erkunden Sie Tutorials, laden Sie Tools herunter und erfahren Sie mehr über Veranstaltungen für Entwickler. AWS
- AWS Entwicklertools — Links zu Entwicklertools SDKs, IDE-Toolkits und Befehlszeilentools für die Entwicklung und Verwaltung von AWS Anwendungen.
- Ressourcencenter für die ersten Schritte — Erfahren Sie AWS-Konto, wie Sie Ihre erste Anwendung einrichten, der AWS Community beitreten und sie starten.
- Praktische Tutorials — Folgen Sie den step-by-step Tutorials, um Ihre erste Anwendung zu starten. AWS
- AWS Whitepapers — Links zu einer umfassenden Liste von technischen AWS Whitepapers zu Themen wie Architektur, Sicherheit und Wirtschaft, die von Solutions Architects oder anderen technischen Experten verfasst wurden. AWS
- AWS -Support Center — Die zentrale Anlaufstelle für die Erstellung und Verwaltung Ihrer Fälle. AWS -Support Enthält auch Links zu anderen hilfreichen Ressourcen wie Foren, technischen FAQs Informationen, Servicestatus und AWS Trusted Advisor.
- Support— Die wichtigste Webseite mit Informationen über Support einen Support-Kanal mit schnellen Reaktionszeiten one-on-one, der Sie bei der Entwicklung und Ausführung von Anwendungen in der Cloud unterstützt.
- Kontakt – Zentraler Kontaktpunkt für Fragen zu AWS -Abrechnung, Konten, Ereignissen Missbrauch und anderen Problemen.
- AWS Nutzungsbedingungen der Website — Detaillierte Informationen zu unseren Urheberrechten und Marken, zu Ihrem Konto, Ihrer Lizenz und Ihrem Zugriff auf die Website sowie zu anderen Themen.

Voraussetzungen

Um als WorkMail Amazon-Administrator zu agieren, benötigen Sie ein AWS-Konto. Wenn Sie sich noch nicht für AWS angemeldet haben, gehen Sie wie folgt vor, um ein Konto einzurichten.

Themen

- Melden Sie sich an für ein AWS-Konto
- Erstellen eines Benutzers mit Administratorzugriff
- Erteilen Sie IAM-Benutzerberechtigungen für Amazon WorkMail

Melden Sie sich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

   Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscodes auf der Telefontastatur.

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

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können Ihre aktuellen Kontoaktivitäten jederzeit einsehen und Ihr Konto verwalten, indem Sie zu https://aws.amazon.com/gehen und Mein Konto auswählen.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Erteilen Sie IAM-Benutzerberechtigungen für Amazon WorkMail

Standardmäßig sind IAM-Benutzer nicht berechtigt, WorkMail Amazon-Ressourcen zu verwalten. Sie müssen eine von AWS verwaltete Richtlinie (AmazonWorkMailFullAccessoder AmazonWorkMailReadOnlyAccess) anhängen oder eine vom Kunden verwaltete Richtlinie erstellen, die IAM-Benutzern diese Berechtigungen ausdrücklich gewährt. Ordnen Sie dann diese Richtlinie den IAM-Benutzern oder -Gruppen zu, die diese Berechtigungen benötigen. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon WorkMail.

Sicherheit bei Amazon WorkMail

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon gelten WorkMail, finden Sie unter AWS Services in Scope by Compliance Program.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung von Amazon anwenden können WorkMail. In den folgenden Themen erfahren Sie, wie Sie Amazon konfigurieren WorkMail , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS-Services nutzen können, die Sie bei der Überwachung und Sicherung Ihrer WorkMail Amazon-Ressourcen unterstützen.

Themen

- Datenschutz bei Amazon WorkMail
- Identitäts- und Zugriffsmanagement für Amazon WorkMail
- AWS verwaltete Richtlinien für Amazon WorkMail
- Verwenden von serviceverknüpften Rollen für Amazon WorkMail
- Protokollierung und Überwachung in Amazon WorkMail
- Konformitätsvalidierung für Amazon WorkMail
- Resilienz bei Amazon WorkMail
- Infrastruktursicherheit bei Amazon WorkMail

Datenschutz bei Amazon WorkMail

Das AWS Modell der gilt für den Datenschutz bei Amazon WorkMail. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon WorkMail oder anderen zusammenarbeiten und die Konsole AWS CLI, API oder AWS-Services verwenden AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

So WorkMail nutzt Amazon AWS KMS

Amazon verschlüsselt WorkMail transparent alle Nachrichten in den Postfächern aller WorkMail Amazon-Organisationen, bevor die Nachrichten auf die Festplatte geschrieben werden, und es entschlüsselt die Nachrichten transparent, wenn Benutzer darauf zugreifen. Sie können die Verschlüsselung nicht deaktivieren. Um die Verschlüsselungsschlüssel zu schützen, die die Nachrichten schützen, WorkMail ist Amazon in AWS Key Management Service (AWS KMS) integriert.

Amazon bietet WorkMail auch eine Option, mit der Benutzer signierte oder verschlüsselte E-Mails senden können. Diese Verschlüsselungsfunktion verwendet nicht AWS KMS. Weitere Informationen finden Sie unter Enabling signed or encrypted email.

Themen

- WorkMail Amazon-Verschlüsselung
- Autorisieren der Nutzung eines CMKs
- WorkMail Amazon-Verschlüsselungskontext
- Überwachung der WorkMail Amazon-Interaktion mit AWS KMS

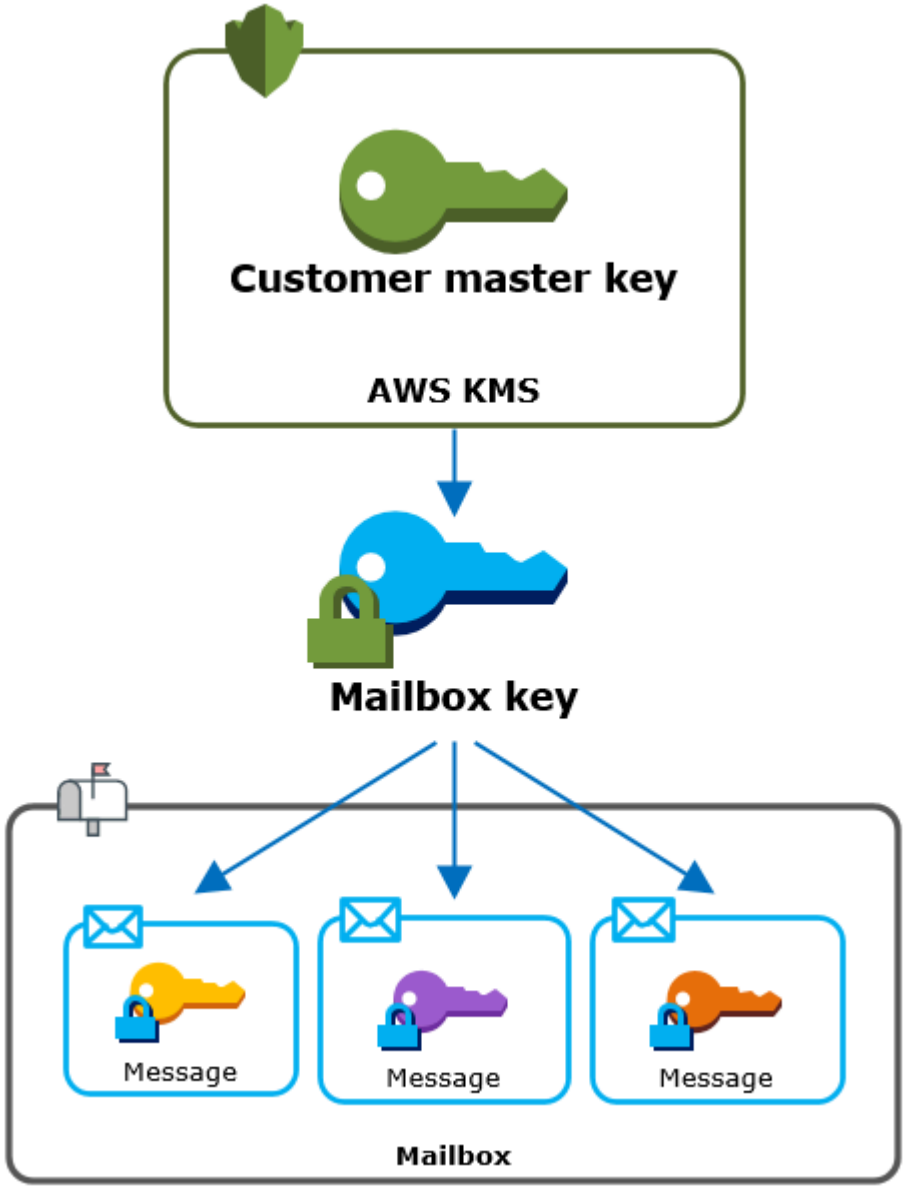
WorkMail Amazon-Verschlüsselung

In Amazon WorkMail kann jede Organisation mehrere Postfächer enthalten, eines für jeden Benutzer in der Organisation. Alle Nachrichten, einschließlich E-Mail und Kalender, werden im Postfach des Benutzers gespeichert.

Um den Inhalt der Postfächer in Ihren WorkMail Amazon-Organisationen zu schützen, WorkMail verschlüsselt Amazon alle Postfachnachrichten, bevor sie auf die Festplatte geschrieben werden. Keine vom Kunden bereitgestellten Informationen werden als Klartext gespeichert.

Jede Nachricht wird mit einem eindeutigen Datenverschlüsselungsschlüssel verschlüsselt. Der Nachrichtenschlüssel wird durch einen Postfach-Schlüssel geschützt. Dabei handelt es sich um einen eindeutigen Verschlüsselungsschlüssel, der nur für das Postfach verwendet wird. Der Postfachschlüssel wird unter einem AWS KMS Kundenhauptschlüssel (CMK) für das Unternehmen verschlüsselt, der ihn niemals unverschlüsselt verlässt. AWS KMS Das folgende Diagramm zeigt die

Beziehung zwischen den verschlüsselten Nachrichten, den verschlüsselten Nachrichtenschlüsseln, dem verschlüsselten Postfach-Schlüssel und dem CMK für die Organisation in AWS KMS auf.



Einrichtung eines CMK für die Organisation

Wenn Sie eine WorkMail Amazon-Organisation erstellen, haben Sie die Möglichkeit, einen AWS KMS Kundenhauptschlüssel (CMK) für die Organisation auszuwählen. Dieser CMK schützt alle Postfach-Schlüssel in dieser Organisation.

Sie können das standardmäßige AWS verwaltete CMK für Amazon auswählen WorkMail, oder Sie können ein vorhandenes, von Kunden verwaltetes CMK auswählen, das Sie besitzen und verwalten. Weitere Informationen finden Sie unter Kundenhauptschlüssel (CMKs) im AWS Key Management

Service Entwicklerhandbuch. Sie können für jede Ihrer Organisationen dasselbe oder ein anderes CMK auswählen, aber Sie können das CMK nicht mehr ändern, wenn Sie es einmal ausgewählt haben.

> **Important**
>
> Amazon WorkMail unterstützt nur symmetrisch CMKs. Sie können kein asymmetrisches CMK verwenden. Hilfe bei der Bestimmung, ob ein CMK symmetrisch oder asymmetrisch ist, finden Sie unter Identifizieren von symmetrisch und asymmetrisch im Entwicklerhandbuch. CMKs AWS Key Management Service

Um den CMK für Ihre Organisation zu finden, verwenden Sie den AWS CloudTrail Protokolleintrag, in dem Anrufe aufgezeichnet werden. AWS KMS

Ein eindeutiger Verschlüsselungsschlüssel für jedes Postfach

Wenn Sie ein Postfach erstellen, WorkMail generiert Amazon außerhalb von einen eindeutigen symmetrischen 256-Bit-AES-Verschlüsselungsschlüssel (Advanced Encryption Standard) für das Postfach, der als Postfachschlüssel bezeichnet wird. AWS KMS Amazon WorkMail verwendet den Postfachschlüssel, um die Verschlüsselungsschlüssel für jede Nachricht im Postfach zu schützen.

Um den Postfachschlüssel zu schützen, WorkMail ruft Amazon AWS KMS dazu auf, den Postfachschlüssel unter dem CMK für die Organisation zu verschlüsseln. Anschließend wird der verschlüsselte Postfach-Schlüssel in den Postfach-Metadaten gespeichert.

> **Note**
>
> Amazon WorkMail verwendet einen symmetrischen Postfach-Verschlüsselungsschlüssel, um Nachrichtenschlüssel zu schützen. Zuvor WorkMail schützte Amazon jedes Postfach mit einem asymmetrischen key pair. Der öffentliche Schlüssel wurde zum Verschlüsseln einzelner Nachrichtenschlüssel verwendet und der private Schlüssel, um sie zu entschlüsseln. Der private Postfach-Schlüssel wurde durch den CMK der Organisation geschützt. Ältere Postfächer verwenden möglicherweise ein asymmetrisches Postfachschlüsselpaar. Diese Änderung hat keine Auswirkungen auf die Sicherheit des Postfachs oder seiner Nachrichten.

Jede Nachricht wird verschlüsselt

Wenn ein Benutzer eine Nachricht zu einem Postfach hinzufügt, WorkMail generiert Amazon einen eindeutigen symmetrischen 256-Bit-AES-Verschlüsselungsschlüssel für die Nachricht außerhalb von. AWS KMS Es verwendet diesen Nachrichtenschlüssel, um die Nachricht zu verschlüsseln. Amazon WorkMail verschlüsselt den Nachrichtenschlüssel unter dem Postfachschlüssel und speichert den verschlüsselten Nachrichtenschlüssel zusammen mit der Nachricht. Anschließend wird der Postfach-Schlüssel mit dem CMK der Organisation verschlüsselt.

Erstellen eines neuen Postfachs

Wenn Amazon ein Postfach WorkMail erstellt, verwendet es den folgenden Prozess, um das Postfach für verschlüsselte Nachrichten vorzubereiten.

- Amazon WorkMail generiert einen eindeutigen symmetrischen 256-Bit-AES-Verschlüsselungsschlüssel für das Postfach außerhalb von AWS KMS.
- Amazon WorkMail ruft den Vorgang AWS KMS Encrypt auf. Dabei werden der Postfachschlüssel und die Kennung des Kundenhauptschlüssels (CMK) für die Organisation übergeben. AWS KMS gibt einen Chiffretext des Postfachschlüssels zurück, der unter dem CMK verschlüsselt wurde.
- Amazon WorkMail speichert den verschlüsselten Postfachschlüssel mit den Postfach-Metadaten.

Verschlüsseln einer Postfach-Nachricht

Um eine Nachricht zu verschlüsseln, WorkMail verwendet Amazon den folgenden Prozess.

1. Amazon WorkMail generiert einen eindeutigen symmetrischen 256-Bit-AES-Schlüssel für die Nachricht. Es verwendet den Klartext-Nachrichtenschlüssel und den Advanced Encryption Standard (AES) -Algorithmus, um die Nachricht außerhalb von zu verschlüsseln. AWS KMS
2. Um den Nachrichtenschlüssel unter dem Postfachschlüssel zu schützen, WorkMail muss Amazon den Postfachschlüssel entschlüsseln, der immer in seiner verschlüsselten Form gespeichert wird.

   Amazon WorkMail ruft den AWS KMS Decrypt-Vorgang auf und übergibt den verschlüsselten Postfachschlüssel. AWS KMS verwendet das CMK für die Organisation, um den Postfachschlüssel zu entschlüsseln, und gibt den Klartext-Postfachschlüssel an Amazon zurück. WorkMail
3. Amazon WorkMail verwendet den Klartext-Postfachschlüssel und den Advanced Encryption Standard (AES) -Algorithmus, um den Nachrichtenschlüssel außerhalb von zu verschlüsseln. AWS KMS

4. Amazon WorkMail speichert den verschlüsselten Nachrichtenschlüssel in den Metadaten der verschlüsselten Nachricht, sodass er für die Entschlüsselung verfügbar ist.

Entschlüsseln einer Postfach-Nachricht

Um eine Nachricht zu entschlüsseln, WorkMail verwendet Amazon den folgenden Prozess.

1. Amazon WorkMail ruft den AWS KMS Decrypt-Vorgang auf und übergibt den verschlüsselten Postfachschlüssel. AWS KMS verwendet das CMK für die Organisation, um den Postfachschlüssel zu entschlüsseln, und gibt den Klartext-Postfachschlüssel an Amazon zurück. WorkMail
2. Amazon WorkMail verwendet den Klartext-Postfachschlüssel und den Advanced Encryption Standard (AES) -Algorithmus, um den verschlüsselten Nachrichtenschlüssel außerhalb von zu entschlüsseln. AWS KMS
3. Amazon WorkMail verwendet den Klartext-Nachrichtenschlüssel, um die verschlüsselte Nachricht zu entschlüsseln.

Zwischenspeichern von Postfachschlüsseln

Um die Leistung zu verbessern und die Anzahl der Anrufe zu minimieren AWS KMS, WorkMail speichert Amazon jeden Klartext-Postfachschlüssel für jeden Kunden lokal für bis zu eine Minute. Am Ende des Caching-Zeitraums wird der Postfach-Schlüssel entfernt. Wenn der Postfachschlüssel für diesen Client während des Caching-Zeitraums benötigt wird, WorkMail kann Amazon ihn aus dem Cache abrufen, anstatt ihn aufzurufen AWS KMS. Der Postfach-Schlüssel wird im Cache geschützt und wird nie als Klartext auf den Datenträger geschrieben.

Autorisieren der Nutzung eines CMKs

Wenn Amazon einen Customer Master Key (CMK) für kryptografische Operationen WorkMail verwendet, handelt es im Namen des Postfachadministrators.

Um den AWS KMS Kundenhauptschlüssel (CMK) für ein Geheimnis in Ihrem Namen zu verwenden, muss der Administrator über die folgenden Berechtigungen verfügen. Sie können diese erforderlichen Berechtigungen in einer IAM-Richtlinie oder einer Schlüsselrichtlinie festlegen.

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

Damit der CMK nur für Anfragen verwendet werden kann, die von Amazon stammen WorkMail, können Sie den ViaService Bedingungsschlüssel kms: mit dem `workmail.<region>.amazonaws.com` Wert verwenden.

Sie können auch die Schlüssel oder Werte im Verschlüsselungskontext als Bedingung für die Verwendung des CMK für kryptografische Operationen verwenden. Sie können beispielsweise einen Zeichenfolgen-Bedingungsoperator in einem IAM- oder Schlüsselrichtliniendokument oder eine Erteilungseinschränkung in einer Erteilung verwenden.

Schlüsselrichtlinie für die von AWS verwaltete CMK

Die Schlüsselrichtlinie für das AWS verwaltete CMK für Amazon WorkMail gibt Benutzern nur dann die Erlaubnis, das CMK für bestimmte Operationen zu verwenden, wenn Amazon die Anfrage im Namen des Benutzers WorkMail stellt. Die Schlüsselrichtlinie erlaubt es keinem Benutzer, den CMK direkt zu verwenden.

Diese Schlüsselrichtlinie wird – wie die Richtlinien aller AWS -verwalteten Schlüssel – vom Service eingerichtet. Sie können die Schlüsselrichtlinie nicht ändern, aber Sie können sie jederzeit einsehen. Einzelheiten finden Sie im AWS Key Management Service Entwicklerhandbuch unter Wichtige Richtlinien anzeigen.

Die Richtlinienanweisungen in der Schlüsselrichtlinie haben folgende Wirkungen:

- Erlauben Sie Benutzern im Konto und in der Region, das CMK für kryptografische Operationen zu verwenden und Zuschüsse zu erstellen, aber nur, wenn die Anfrage von WorkMail Amazon in ihrem Namen kommt. Der Bedingungsschlüssel `kms:ViaService` setzt diese Beschränkung durch.
- Ermöglicht es dem AWS Konto, IAM-Richtlinien zu erstellen, die es Benutzern ermöglichen, CMK-Eigenschaften einzusehen und Zuschüsse zu widerrufen.

Im Folgenden finden Sie eine wichtige Richtlinie für ein Beispiel für ein AWS verwaltetes CMK für Amazon WorkMail.

```
{
  "Version" : "2012-10-17",
  "Id" : "auto-workmail-1",
  "Statement" : [ {
    "Sid" : "Allow access through WorkMail for all principals in the account that are
 authorized to use WorkMail",
```

```
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [ "kms:Decrypt", "kms:CreateGrant", "kms:ReEncrypt*", "kms:DescribeKey",
 "kms:Encrypt" ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "workmail.us-east-1.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
    }
  }, {
    "Sid" : "Allow direct access to key metadata to the account",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [ "kms:Describe*", "kms:List*", "kms:Get*", "kms:RevokeGrant" ],
    "Resource" : "*"
  } ]
}
```

Verwendung von Zuschüssen zur Autorisierung von Amazon WorkMail

Zusätzlich zu den wichtigsten Richtlinien WorkMail verwendet Amazon Zuschüsse, um dem CMK für jede Organisation Berechtigungen hinzuzufügen. Verwenden Sie den Vorgang, um die Zuschüsse auf dem CMK in Ihrem Konto ListGrantseinzusehen.

Amazon WorkMail verwendet Zuschüsse, um dem CMK für die Organisation die folgenden Berechtigungen hinzuzufügen.

- Fügen Sie die `kms:Encrypt` Erlaubnis hinzu, Amazon die Verschlüsselung des Postfachschlüssels WorkMail zu gestatten.
- Fügen Sie die `kms:Decrypt` Berechtigung hinzu, damit Amazon den CMK WorkMail zum Entschlüsseln des Postfachschlüssels verwenden kann. Amazon WorkMail benötigt diese Berechtigung im Rahmen einer Erteilung, da die Anforderung zum Lesen von Postfachnachrichten den Sicherheitskontext des Benutzers verwendet, der die Nachricht liest. Die Anfrage verwendet nicht die Anmeldeinformationen des AWS Kontos. Amazon WorkMail gewährt diesen Zuschuss, wenn Sie einen CMK für die Organisation auswählen.

Um die Zuschüsse zu erstellen, WorkMail ruft CreateGrantAmazon im Namen des Benutzers an, der die Organisation erstellt hat. Die Berechtigung zum Erstellen der Erteilung stammt aus der Schlüsselrichtlinie. Diese Richtlinie ermöglicht es Kontobenutzern, `CreateGrant` den CMK für die Organisation anzurufen, wenn Amazon die Anfrage im Namen eines autorisierten Benutzers WorkMail stellt.

Die Schlüsselrichtlinie ermöglicht es dem Kontoinhaber auch, die Gewährung des AWS verwalteten Schlüssels zu widerrufen. Wenn Sie den Zuschuss widerrufen, WorkMail kann Amazon die verschlüsselten Daten in Ihren Postfächern jedoch nicht entschlüsseln.

WorkMail Amazon-Verschlüsselungskontext

Ein Verschlüsselungskontext ist eine Gruppe von Schlüssel/Wert-Paaren mit zufälligen, nicht geheimen Daten. Wenn Sie einen Verschlüsselungskontext in eine Anfrage zur Verschlüsselung von Daten aufnehmen, wird der Verschlüsselungskontext AWS KMS kryptografisch an die verschlüsselten Daten gebunden. Zur Entschlüsselung der Daten müssen Sie denselben Verschlüsselungskontext übergeben. Weitere Informationen finden Sie unter Verschlüsselungskontext im AWS Key Management Service -Entwicklerhandbuch.

Amazon WorkMail verwendet bei allen AWS KMS kryptografischen Vorgängen dasselbe Verschlüsselungskontextformat. Sie können eine kryptografische Operation in Prüfungsdatensätzen und -Protokollen wie AWS CloudTrail anhand des Verschlüsselungskontexts identifizieren. Dieser kann auch als Bedingung für die Autorisierung in Richtlinien und Erteilungen verwendet werden.

In seinen Encrypt and Decrypt-Anfragen an WorkMail verwendet Amazon einen Verschlüsselungskontext AWS KMS, in dem sich der Schlüssel befindet `aws:workmail:arn` und der Wert dem Amazon-Ressourcennamen (ARN) der Organisation entspricht.

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization-ID"
```

Der folgende Verschlüsselungskontext umfasst beispielsweise einen Beispiel-Organisations-ARN in der Region Europa (Irland`eu-west-1`) ().

```
"aws:workmail:arn":"arn:aws:workmail:eu-west-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
```

Überwachung der WorkMail Amazon-Interaktion mit AWS KMS

Sie können Amazon AWS CloudTrail CloudWatch Logs verwenden, um die Anfragen zu verfolgen, an die Amazon in AWS KMS Ihrem Namen WorkMail sendet.

Encrypt

Wenn Sie ein Postfach erstellen, WorkMail generiert Amazon einen Postfachschlüssel und ruft AWS KMS zur Verschlüsselung des Postfachschlüssels auf. Amazon WorkMail sendet eine Encrypt-Anfrage AWS KMS mit dem Klartext-Postfachschlüssel und einer Kennung für das CMK der Amazon-Organisation an. WorkMail

Das Ereignis, das die `Encrypt`-Operation aufzeichnet, ähnelt dem folgenden Beispielereignis. Der Benutzer ist der WorkMail Amazon-Dienst. Zu den Parametern gehören die CMK-ID (`keyId`) und der Verschlüsselungskontext für die WorkMail Amazon-Organisation. Amazon gibt WorkMail auch den Postfachschlüssel weiter, der jedoch nicht im CloudTrail Protokoll aufgezeichnet wird.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestID": "76e96b96-7e24-4faf-a2d6-08ded2eaf63c",
    "eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```

Decrypt

Wenn Sie eine Postfachnachricht hinzufügen, anzeigen oder löschen, WorkMail bittet Amazon darum, den Postfachschlüssel AWS KMS zu entschlüsseln. Amazon WorkMail sendet eine Decrypt-Anfrage AWS KMS mit dem verschlüsselten Postfachschlüssel und einer Kennung für das CMK der WorkMail Amazon-Organisation an.

Das Ereignis, das die `Decrypt`-Operation aufzeichnet, ähnelt dem folgenden Beispielereignis. Der Benutzer ist der WorkMail Amazon-Dienst. Zu den Parametern gehören der verschlüsselte Postfachschlüssel (als Chiffretext-Blob), der nicht im Protokoll aufgezeichnet wird, und der Verschlüsselungskontext für die Amazon-Organisation. WorkMail AWS KMS leitet die ID des CMK aus dem Chiffretext ab.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-20T11:51:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        }
    },
    "responseElements": null,
    "requestID": "4a32dda1-34d9-4100-9718-674b8e0782c9",
    "eventID": "ea9fd966-98e9-4b7b-b377-6e5a397a71de",
    "readOnly": true,
    "resources": [
```

```
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "241e1e5b-ff64-427a-a5b3-7949164d0214"
}
```

Identitäts- und Zugriffsmanagement für Amazon WorkMail

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um WorkMail Amazon-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So WorkMail arbeitet Amazon mit IAM
- Beispiele für WorkMail identitätsbasierte Richtlinien von Amazon
- Fehlerbehebung Amazon WorkMail Amazon-Identität und -Zugriff

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie bei Amazon WorkMail ausführen.

Servicebenutzer — Wenn Sie den WorkMail Amazon-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr WorkMail Amazon-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen,

wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie auf eine Funktion in Amazon nicht zugreifen können WorkMail, finden Sie weitere Informationen unterFehlerbehebung Amazon WorkMail Amazon-Identität und -Zugriff.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die WorkMail Amazon-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon WorkMail. Es ist Ihre Aufgabe, zu bestimmen, auf welche WorkMail Amazon-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Amazon nutzen kann WorkMail, finden Sie unterSo WorkMail arbeitet Amazon mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon zu verwalten. WorkMail Beispiele für WorkMail identitätsbasierte Amazon-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für WorkMail identitätsbasierte Richtlinien von Amazon

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden,

müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto.

Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der

identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So WorkMail arbeitet Amazon mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon zu verwalten WorkMail, sollten Sie wissen, welche IAM-Funktionen für Amazon verfügbar sind. WorkMail Einen allgemeinen Überblick darüber, wie Amazon WorkMail und andere AWS Dienste mit IAM zusammenarbeiten, finden Sie im IAM-Benutzerhandbuch unter AWS Services, die mit IAM funktionieren.

Themen

- WorkMailIdentitätsbasierte Richtlinien von Amazon
- WorkMailRessourcenbasierte Richtlinien von Amazon
- Autorisierung basierend auf WorkMail Amazon-Tags
- Amazon WorkMail IAM-Rollen

WorkMailIdentitätsbasierte Richtlinien von Amazon

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Amazon WorkMail unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Amazon WorkMail verwenden vor der Aktion das folgende Präfix:`workmail:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, eine Liste von Benutzern mit dem WorkMail `ListUsers` Amazon-API-Vorgang abzurufen, nehmen Sie die `workmail:ListUsers` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Amazon WorkMail definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [
      "workmail:ListUsers",
      "workmail:DeleteUser"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

```
"Action": "workmail:List*"
```

Eine Liste der WorkMail Amazon-Aktionen finden Sie unter Von Amazon definierte Aktionen WorkMail im IAM-Benutzerhandbuch.

Ressourcen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Amazon WorkMail unterstützt Berechtigungen auf Ressourcenebene für WorkMail Amazon-Organisationen.

Die WorkMail Amazon-Organisationsressource hat den folgenden ARN:

```
arn:aws:workmail:${Region}:${Account}:organization/${OrganizationId}
```

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs) und AWS Service Namespaces.

Wenn Sie beispielsweise die `m-n1pq2345678r901st2u3vx45x6789yza`-Organisation in Ihrer Anweisung angeben möchten, verwenden Sie den folgenden ARN.

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza"
```

Um alle Organisationen anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/*"
```

Einige WorkMail Amazon-Aktionen, z. B. zum Erstellen von Ressourcen, können nicht für eine bestimmte Ressource ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "*"
```

Eine Liste der WorkMail Amazon-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von Amazon definierte Ressourcen WorkMail im IAM-Benutzerhandbuch. Informationen dazu, mit welchen Aktionen Sie den ARN der einzelnen Ressourcen angeben können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkMail.

Bedingungsschlüssel

Amazon WorkMail unterstützt die folgenden globalen Bedingungsschlüssel.

- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:MultiFactorAuthAge`

- aws:MultiFactorAuthPresent
- aws:PrincipalOrgID
- aws:PrincipalArn
- aws:RequestedRegion
- aws:SecureTransport
- aws:UserAgent

Die folgende Beispielrichtlinie gewährt Zugriff auf die WorkMail Amazon-Konsole nur von MFA-authentifizierten IAM-Prinzipalen in der AWS-Region. eu-west-1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:Describe*",
                "ses:Get*",
                "workmail:Describe*",
                "workmail:Get*",
                "workmail:List*",
                "workmail:Search*",
                "lambda:ListFunctions",
                "iam:ListRoles",
                "logs:DescribeLogGroups",
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "Bool": {
                    "aws:MultiFactorAuthPresent": true
                }
            }
        }
    ]
```

```
}
```

Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

`workmail:ImpersonationRoleId`ist der einzige servicespezifische Bedingungsschlüssel, der von Amazon WorkMail unterstützt wird.

In der folgenden Beispielrichtlinie wird die `AssumeImpersonationRole` Aktion auf eine bestimmte WorkMail Organisation und eine bestimmte Rolle, die sich ausgibt, beschränkt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workmail:AssumeImpersonationRole"
      ],
      "Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza",
      "Condition": {
        "StringEquals": {
          "workmail:ImpersonationRoleId":"12345678-1234-1234-1234-123456789012"
        }
      }
    }
  ]
}
```

Beispiele

Beispiele für WorkMail identitätsbasierte Richtlinien von Amazon finden Sie unter. Beispiele für WorkMail identitätsbasierte Richtlinien von Amazon

WorkMailRessourcenbasierte Richtlinien von Amazon

Amazon unterstützt WorkMail keine ressourcenbasierten Richtlinien.

Autorisierung basierend auf WorkMail Amazon-Tags

Sie können Tags an WorkMail Amazon-Ressourcen anhängen oder Tags in einer Anfrage an Amazon weitergeben WorkMail. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden. Weitere Informationen zum Taggen von WorkMail Amazon-Ressourcen finden Sie unterMarkieren einer Organisation.

Amazon WorkMail IAM-Rollen

Eine IAM-Rolle ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Temporäre Anmeldeinformationen mit Amazon verwenden WorkMail

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder aufrufen GetFederationToken.

Amazon WorkMail unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen durchzuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Amazon WorkMail unterstützt serviceverknüpfte Rollen. Einzelheiten zum Erstellen oder Verwalten von Rollen, die mit dem Service von WorkMail Amazon verknüpft sind, finden Sie unterVerwenden von serviceverknüpften Rollen für Amazon WorkMail.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto.

Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Amazon WorkMail unterstützt Servicerollen.

Beispiele für WorkMail identitätsbasierte Richtlinien von Amazon

Standardmäßig sind IAM-Benutzer und -Rollen nicht berechtigt, WorkMail Amazon-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der WorkMail Amazon-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Erlauben Sie Benutzern nur Lesezugriff auf Amazon-Ressourcen WorkMail

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand WorkMail Amazon-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden

Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der WorkMail Amazon-Konsole

Um auf die WorkMail Amazon-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den WorkMail Amazon-Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Benutzer oder -Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten weiterhin die WorkMail Amazon-Konsole verwenden können, fügen Sie den Entitäten auch die folgende AWS verwaltete Richtlinie hinzu. AmazonWorkMailFullAccess Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Die AmazonWorkMailFullAccessRichtlinie gewährt einem IAM-Benutzer vollen Zugriff auf WorkMail Amazon-Ressourcen. Diese Richtlinie gewährt dem Benutzer Zugriff auf alle Amazon WorkMail AWS Key Management Service, Amazon Simple Email Service und AWS Directory Service Operationen. Dazu gehören auch mehrere EC2 Amazon-Operationen, die Amazon in Ihrem Namen durchführen WorkMail muss. Die `cloudwatch` Berechtigungen `logs` und sind für die Protokollierung von E-Mail-Ereignissen und die Anzeige von Metriken in der WorkMail Amazon-Konsole erforderlich. Die Audit-Protokollierung verwendet CloudWatch Logs, Amazon S3 und Amazon-Daten FireHose zum Speichern`logs`. Weitere Informationen finden Sie unter Protokollierung und Überwachung in Amazon WorkMail.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailAdministration",
      "Effect": "Allow",
      "Action": [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DeleteDeliveryDestination",
        "logs:DeleteDeliveryDestinationPolicy",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliveryDestinationPolicy",
        "logs:CreateDelivery",
        "logs:DeleteDelivery",
        "logs:DescribeDeliveries",
        "logs:GetDelivery",
        "logs:DeleteDeliverySource",
        "logs:DescribeDeliverySources",
```

```
            "logs:GetDeliverySource",
            "logs:PutDeliverySource",
            "logs:DescribeResourcePolicies",
            "cloudwatch:GetMetricData",
            "firehose:DescribeDeliveryStream",
            "firehose:ListDeliveryStreams",
            "s3:ListAllMyBuckets"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AuditLogDeliveryThroughCWLogs",
        "Effect": "Allow",
        "Action": [
            "firehose:TagDeliveryStream",
            "logs:PutResourcePolicy",
            "s3:GetBucketPolicy",
            "s3:PutBucketPolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:CalledViaLast": "logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "events.workmail.amazonaws.com"
            }
        }
    },
    {
        "Sid": "AuditLoggingLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
```

```
                "iam:AWSServiceName": "delivery.logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsUnlink",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/
events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
        "Sid": "InboundOutboundEmailEventsAuth",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::*:role/*workmail*",
        "Condition": {
            "StringLike": {
                "iam:PassedToService": "events.workmail.amazonaws.com"
            }
        }
    }
  ]
}
```

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

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

```
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Erlauben Sie Benutzern nur Lesezugriff auf Amazon-Ressourcen WorkMail

Die folgende Grundsatzerklärung gewährt einem IAM-Benutzer nur Lesezugriff auf Amazon-Ressourcen. WorkMail Diese Richtlinie bietet dieselbe Zugriffsebene wie die von AWS verwaltete Richtlinie AmazonWorkMailReadOnlyAccess. Beide Richtlinien gewähren dem Benutzer Zugriff auf alle WorkMail `Describe` Amazon-Operationen. Der Zugriff auf den AWS Directory Service `DescribeDirectories` Vorgang ist erforderlich, um Informationen über Ihre AWS Directory Service Verzeichnisse zu erhalten. Zugriff auf den Amazon SES SES-Service ist erforderlich, um Informationen über die konfigurierten Domains zu erhalten. Zugriff auf AWS Key Management Service ist erforderlich, um Informationen über die verwendeten Verschlüsselungsschlüssel zu erhalten. Die `cloudwatch` Berechtigungen `logs` und sind für die Protokollierung von E-Mail-

Ereignissen und die Anzeige von Metriken in der WorkMail Amazon-Konsole erforderlich. Die Audit-Protokollierung verwendet CloudWatch Logs, Amazon S3 und Amazon-Daten FireHose zum Speichern`logs`. Weitere Informationen finden Sie unter Protokollierung und Überwachung in Amazon WorkMail.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailReadOnly",
      "Effect": "Allow",
      "Action": [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliverySources",
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
    }
  ]
}
```

Fehlerbehebung Amazon WorkMail Amazon-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon WorkMail und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Amazon durchzuführen WorkMail

- Ich bin nicht berechtigt, IAM auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine WorkMail Amazon-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in Amazon durchzuführen WorkMail

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zu verwenden, um Details zu einer Gruppe anzuzeigen, aber nicht über die `workmail:DescribeGroup` entsprechenden Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workmail:DescribeGroup on resource: group
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion `group` auf die Ressource `workmail:DescribeGroup` zugreifen zu können.

Ich bin nicht berechtigt, IAM auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon weitergeben können WorkMail.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon WorkMail auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine WorkMail Amazon-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon diese Funktionen WorkMail unterstützt, finden Sie unterSo WorkMail arbeitet Amazon mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Bereitstellen von Zugriff für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für Amazon WorkMail

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien

verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS verwaltete Richtlinie: AmazonWorkMailFullAccess

Sie können die `AmazonWorkMailFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die den vollen Zugriff auf Amazon ermöglichen WorkMail.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AmazonWorkMailFullAccess im AWS Management Console.

AWS verwaltete Richtlinie: AmazonWorkMailReadOnlyAccess

Sie können die `AmazonWorkMailReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die nur Lesezugriff auf Amazon ermöglichen. WorkMail

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AmazonWorkMailReadOnlyAccess im AWS Management Console.

AWS verwaltete Richtlinie: AmazonWorkMailEventsServiceRolePolicy

Diese Richtlinie ist der serviceverknüpften Rolle zugeordnet, die benannt wurde AmazonWorkMailEvents, um den Zugriff auf AWS Dienste und Ressourcen zu ermöglichen, die von

WorkMail Amazon-Veranstaltungen genutzt oder verwaltet werden. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon WorkMail.

WorkMail Aktualisierungen der AWS verwalteten Richtlinien durch Amazon

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon an, WorkMail seit dieser Service begonnen hat, diese Änderungen zu verfolgen.

Änderung	Beschreibung	Datum
Von AWS verwaltete Richtlinienaktualisierungen — Aktualisierung einer bestehenden Richtlinie	Die `AmazonWorkMailFullAccess` Berechtigungen `AmazonWorkMailReadOnlyAccess` und wurden für Amazon aktualisiert WorkMail , um die Auditprotokollierung zu unterstützen. Weitere Informationen zu den aktualisierten Berechtigungen finden Sie unter Beispiele für WorkMail identitätsbasierte Richtlinien von Amazon und Informationen zur Auditprotokollierung finden Sie unterAudit-Protokollierung aktivieren.	14. Februar 2024
Amazon WorkMail hat begonnen, Änderungen zu verfolgen	Amazon WorkMail hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	1. März 2021

Verwenden von serviceverknüpften Rollen für Amazon WorkMail

Amazon WorkMail verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon verknüpft

ist. WorkMail Servicebezogene Rollen sind von Amazon vordefiniert WorkMail und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle WorkMail erleichtert die Einrichtung von Amazon, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon WorkMail definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, WorkMail kann nur Amazon seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle nur löschen, nachdem Sie zuvor die zugehörigen Ressourcen gelöscht haben. Dies schützt Ihre WorkMail Amazon-Ressourcen, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entziehen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Servicebezogene Rollenberechtigungen für Amazon WorkMail

Amazon WorkMail verwendet die serviceverknüpfte Rolle mit dem Namen AmazonWorkMailEvents—Amazon WorkMail verwendet diese servicebezogene Rolle, um den Zugriff auf AWS Dienste und Ressourcen zu ermöglichen, die von WorkMail Amazon-Ereignissen verwendet oder verwaltet werden, wie z. B. die Überwachung von E-Mail-Ereignissen, die von protokolliert wurden. CloudWatch Weitere Informationen zur Aktivierung der E-Mail-Ereignisprotokollierung für Amazon WorkMail finden Sie unterDie Protokollierung von E-Mail-Ereignissen aktivieren.

Die AmazonWorkMailEvents dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `events.workmail.amazonaws.com`

Die Rollenberechtigungsrichtlinie ermöglicht es Amazon WorkMail , die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `logs:CreateLogGroup` für `all AWS resources`
- Aktion: `logs:CreateLogStream` für `all AWS resources`

- Aktion: `logs:PutLogEvents` für `all AWS resources`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Amazon erstellen WorkMail

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die WorkMail Amazon-Ereignisprotokollierung aktivieren und die Standardeinstellungen in der WorkMail Amazon-Konsole verwenden, WorkMail erstellt Amazon die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie die WorkMail Amazon-Ereignisprotokollierung aktivieren und die Standardeinstellungen verwenden, WorkMail erstellt Amazon die serviceverknüpfte Rolle erneut für Sie.

Bearbeitung einer serviceverknüpften Rolle für Amazon WorkMail

Amazon WorkMail erlaubt Ihnen nicht, die AmazonWorkMailEvents serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon WorkMail

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der WorkMail Amazon-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um WorkMail Amazon-Ressourcen zu löschen, die verwendet werden von AmazonWorkMailEvents

1. Schalten Sie die WorkMail Amazon-Ereignisprotokollierung aus.
   a. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

      Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
   b. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
   c. Wählen Sie im Navigationsbereich Organisationseinstellungen und dann Überwachung aus.
   d. Wählen Sie für Log settings (Protokolleinstellungen) Edit (Bearbeiten) aus.
   e. Stellen Sie den Schieberegler E-Mail-Ereignisse aktivieren auf die Position Aus.
   f. Wählen Sie Save (Speichern) aus.
2. Löschen Sie die CloudWatch Amazon-Protokollgruppe.
   a. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
   b. Wählen Sie Logs.
   c. Wählen Sie für Log Groups (Protokollgruppen) die zu löschende Protokollgruppe aus.
   d. Wählen Sie für Actions (Aktionen) die Option Delete log group (Protokollgruppe löschen) aus.
   e. Wählen Sie Yes, Delete (Ja, löschen) aus.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AmazonWorkMailEvents serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für Rollen im WorkMail Zusammenhang mit Amazon Services

Amazon WorkMail unterstützt die Verwendung von Rollen im Zusammenhang mit Services in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter WorkMail Amazon-Regionen und -Endpunkte.

Protokollierung und Überwachung in Amazon WorkMail

Die Überwachung und Prüfung Ihrer E-Mails und Protokolle ist wichtig, um die Integrität Ihrer WorkMail Amazon-Organisation aufrechtzuerhalten. Amazon WorkMail unterstützt zwei Arten der Überwachung:

- Ereignisprotokollierung — Die Überwachung der E-Mail-Versandaktivitäten für Ihr Unternehmen trägt zum Schutz Ihrer Domain-Reputation bei. Durch die Überwachung können Sie zudem E-Mails nachverfolgen, die gesendet und empfangen wurden. Weitere Informationen zum Aktivieren der E-Mail-Ereignisprotokollierung finden Sie unter Die Protokollierung von E-Mail-Ereignissen aktivieren.
- Audit-Protokollierung — Sie können Audit-Logs verwenden, um detaillierte Informationen über die Nutzung Ihrer WorkMail Amazon-Organisation zu erfassen, z. B. den Zugriff von Benutzern auf Postfächer zu überwachen, auf verdächtige Aktivitäten zu prüfen und die Konfiguration von Zugriffskontroll- und Verfügbarkeitsanbietern zu debuggen. Weitere Informationen finden Sie unter Audit-Protokollierung aktivieren.

AWS bietet die folgenden Überwachungstools, um Amazon zu beobachten WorkMail, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Wenn Sie beispielsweise die Protokollierung von E-Mail-Ereignissen für Amazon aktivieren WorkMail, CloudWatch können Sie die für Ihr Unternehmen gesendeten und empfangenen E-Mails verfolgen. Weitere Informationen zur Überwachung von Amazon WorkMail mit CloudWatch finden Sie unterAmazon WorkMail mit CloudWatch Metriken überwachen. Weitere Informationen zu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre E-Mail-Ereignisse und Audit-Logs für Amazon überwachen, speichern und darauf zugreifen, WorkMail wenn die E-Mail- und Audit-Protokollierung in der WorkMail Amazon-Konsole aktiviert ist. CloudWatch Mithilfe von Logs können Informationen in den Protokolldateien überwacht werden, und Sie können Ihre Protokolldaten in einem äußerst stabilen Speicher archivieren. Weitere Informationen zur Nachverfolgung von WorkMail Amazon-Nachrichten mithilfe von CloudWatch Logs finden Sie unter Die Protokollierung von E-Mail-Ereignissen aktivieren undAudit-Protokollierung aktivieren. Weitere Informationen zu CloudWatch Logs finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden AWS-Konto, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten

angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie unter Protokollierung Amazon WorkMail Amazon-API-Aufrufen mit AWS CloudTrail.

- Mit Amazon S3 können Sie Ihre WorkMail Amazon-Events auf kostengünstige Weise speichern und darauf zugreifen. Amazon S3 bietet Mechanismen zur Verwaltung des Lebenszyklus von Ereignisdaten, sodass Sie das automatische Löschen alter Ereignisse oder die automatische Archivierung in Amazon S3 Glacier konfigurieren können. Hinweis: Die Lieferung mit Amazon S3 ist nur für Auditprotokollierungsereignisse verfügbar. Weitere Informationen zu Amazon S3 finden Sie im Amazon S3 S3-Benutzerhandbuch.
- Mit Amazon Data Firehose können Sie Ihre Eventdaten an andere AWS-Services wie Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon OpenSearch Service, Amazon OpenSearch Serverless, Splunk und alle benutzerdefinierten HTTP-Endpunkte oder HTTP-Endpunkte streamen, die von unterstützten Drittanbietern wie Datadog, Dynatrace, MongoDB, New Relic, Coralogix und Elastic betrieben werden. LogicMonitor Die Lieferung an Firehose ist nur für Auditprotokollierungsereignisse verfügbar. Weitere Informationen zu Firehose finden Sie im Amazon Data Firehose Developer Guide.

Themen

- Amazon WorkMail mit CloudWatch Metriken überwachen
- Überwachung der WorkMail E-Mail-Ereignisprotokolle von Amazon
- Überwachung der WorkMail Amazon-Auditprotokolle
- CloudWatch Insights mit Amazon verwenden WorkMail
- Protokollierung Amazon WorkMail Amazon-API-Aufrufen mit AWS CloudTrail
- Die Protokollierung von E-Mail-Ereignissen aktivieren
- Audit-Protokollierung aktivieren

Amazon WorkMail mit CloudWatch Metriken überwachen

Sie können Amazon WorkMail mithilfe von Amazon überwachen CloudWatch, das Rohdaten sammelt und sie zu lesbaren, nahezu in Echtzeit verfügbaren Metriken verarbeitet. Die kostenlosen Kennzahlen werden 15 Monate lang gespeichert, sodass Sie auf historische Informationen zugreifen können, um zu sehen, wie Ihre Webanwendung oder Ihr Service funktioniert. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder

Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

CloudWatch Metriken für Amazon WorkMail

Amazon WorkMail sendet die folgenden Kennzahlen und Dimensionsinformationen an CloudWatch.

Der `AWS/WorkMail`-Namespace enthält die folgenden Metriken.

Metrik	Beschreibung
`OrganizationEmailReceived`	Die Anzahl der E-Mails, die Ihre WorkMail Amazon-Organisation erhalten hat. Wenn eine E-Mail an 10 Empfänger in Ihrer Organisation adressiert ist, beträgt die `OrganizationEmailReceived` Anzahl eins. Einheiten: Anzahl
`MailboxEmailDelivered`	Die Anzahl der E-Mails, die an einzelne Postfächer in Ihrer WorkMail Amazon-Organisation zugestellt wurden. Wenn eine E-Mail erfolgreich an 10 Empfänger in Ihrer Organisation zugestellt wurde, beträgt die `MailboxEmailDelivered` Anzahl 10. Einheiten: Anzahl
`IncomingEmailBounced`	Die Anzahl der eingehenden E-Mails, die aufgrund voller Postfächer zurückgewiesen wurden. Diese Metrik wird für jeden beabsichtigten Empfänger erstellt. Wenn beispielsweise eine E-Mail an 10 Empfänger in Ihrer Organisation gesendet wird und zwei der Empfänger volle Postfächer haben, was zu einer Bounce-Antwort führt, beträgt die `IncomingEmailBounced` Anzahl zwei. Einheiten: Anzahl

Metrik	Beschreibung
`OutgoingEmailBounced`	Die Anzahl der ausgehenden E-Mails, die nicht zugestellt werden konnten. Diese Metrik wird für jeden beabsichtigten Empfänger erstellt. Wenn beispielsweise eine E-Mail an 10 Empfänger gesendet wird und zwei E-Mails nicht zugestellt werden konnten, beträgt die `OutgoingEmailBounced` Anzahl 2. Einheiten: Anzahl
`OutgoingEmailSent`	Die Anzahl der erfolgreich von Ihrer WorkMail Amazon-Organisation versendeten E-Mails. Diese Metrik wird für jeden einzelnen Empfänger einer erfolgreich versendeten E-Mail berechnet. Beispiel: Wenn 1 E-Mail an 10 Empfänger gesendet wurde und an 8 Empfänger erfolgreich zugestellt werden konnte, ist die `OutgoingEmailSent` -Anzahl 8. Einheiten: Anzahl

Metrik	Beschreibung
`AuthenticationFailure`	Diese Metrik zählt die Anzahl der Authentif izierungsversuche. Wenn die Authentifizierung erfolgreich ist, ist die Anzahl 0 und wenn die Authentifizierung nicht erfolgreich ist, ist die Anzahl 1. Verwenden Sie die `Sum` Statistik, um die Anzahl der fehlgeschlagenen Authentif izierungsversuche zu überwachen. Verwenden Sie die `Sample count` Statistik, um die Gesamtzahl der Authentifizierungsereignisse zu überwachen. Verwenden Sie die `Average` Statistik, um das Verhältnis von fehlgesch lagenen und erfolgreichen Authentifizierungs ereignissen zu überwachen. Einheiten: Anzahl
`AccessDenied`	Diese Metrik zählt die Anzahl der Bewertung en der Zugriffskontrolle. Wenn die Aktion von der Zugriffskontrolle verweigert wird, beträgt die Anzahl 1, und wenn eine Aktion gewährt wird, ist die Anzahl 0. Verwenden Sie die `Sum` Statistik, um das Volumen der abgelehnten Aktionen zu überwachen, die `Sample count` Statistik, um die Gesamtzahl der versuchten Aktionen zu überwachen, und die `Average` Statistik, um das Verhältnis zwischen erlaubten und abgelehnten Aktionen zu überwachen. Einheiten: Anzahl

Metrik	Beschreibung
`ActionDenied`	Diese Metrik wird gezählt, wenn Aktionen mit den Postfachdaten durchgeführt werden. Wenn die Aktion verweigert wird, beträgt die Anzahl 1, und wenn eine Aktion gewährt wird, ist die Anzahl 0. Verwenden Sie die `Sum` Statistik, um das Volumen der abgelehnten Postfacha ktionen zu überwachen, die `Sample count` Statistik, um die Gesamtzahl der versuchte n Postfachaktionen zu überwachen, und die `Average` Statistik, um das Verhältnis zwischen erlaubten und abgelehnten Aktionen zu überwachen. Einheiten: Anzahl
`AvailabilityProviderFailure`	Diese Metrik wird für jede Anfrage eines Verfügbarkeitsanbieters gezählt, die Amazon WorkMail ausführt, um die Kalenderverfügbark eit von einer externen Quelle abzurufen. Weitere Informationen zu Verfügbarkeitsanbi etern finden Sie im Amazon WorkMail Administr ator Guide.

Überwachung der WorkMail E-Mail-Ereignisprotokolle von Amazon

Wenn Sie die E-Mail-Ereignisprotokollierung für Ihre WorkMail Amazon-Organisation aktivieren, WorkMail protokolliert Amazon E-Mail-Ereignisse mit CloudWatch. Weitere Informationen zum Einschalten der E-Mail-Ereignisprotokollierung finden Sie unter Die Protokollierung von E-Mail-Ereignissen aktivieren.

In den folgenden Tabellen werden die Ereignisse beschrieben, die Amazon WorkMail protokolliert CloudWatch, wann die Ereignisse übertragen werden und was die Ereignisfelder enthalten.

`ORGANIZATION_EMAIL_RECEIVED`

Dieses Ereignis wird protokolliert, wenn Ihre WorkMail Amazon-Organisation eine E-Mail-Nachricht erhält.

Feld	Beschreibung
recipients	Die beabsichtigten Empfänger der Nachricht.
sender	Die E-Mail-Adresse des Benutzers, der die E-Mail-Nachricht im Namen eines anderen Benutzers gesendet hat. Dieses Feld wird nur eingestellt, wenn eine E-Mail im Namen eines anderen Benutzers gesendet wird.
from	Die Adresse für From (Von). Dies ist in der Regel die E-Mail-Adresse des Benutzers, der die Nachricht gesendet hat. Wenn der Benutzer die Nachricht als ein anderer Benutzer oder im Auftrag eines anderen Benutzers gesendet hat, gibt das Feld die E-Mail-Adresse des Benutzers zurück, in dessen Auftrag die E-Mail gesendet wurde, und nicht die E-Mail-Adresse des tatsächlichen Absenders.
subject	Der Betreff der E-Mail-Nachricht.
messageId	Die SMTP-Nachrichten-ID
spamVerdict	Gibt an, ob die Nachricht von Amazon SES als Spam markiert wurde. Weitere Informationen finden Sie unter Inhalt der Benachrichtigungen für den E-Mail-Empfang von Amazon SES im Amazon Simple Email Service Developer Guide.
dkimVerdict	Gibt an, ob die DomainKeys Identified Mail (DKIM) -Prüfung bestanden wurde. Weitere Informationen finden Sie unter Inhalt der Benachrichtigungen für den E-Mail-Empfang

Feld	Beschreibung
	von Amazon SES im Amazon Simple Email Service Developer Guide.
dmarcVerdict	Gibt an, ob die DMARC-Prüfung (Domain-based Message Authentication, Reporting and Conformance) bestanden wurde. Weitere Informationen finden Sie unter Inhalt der Benachrichtigungen für den E-Mail-Empfang von Amazon SES im Amazon Simple Email Service Developer Guide.
dmarcPolicy	Erscheint nur, wenn das dmarcVerdict-Feld „FAIL“ enthält. Gibt die Aktion an, die für die E-Mail ausgeführt werden soll, wenn die DMARC-Prüfung fehlschlägt (NONE, QUARANTINE oder REJECT). Dies wird vom Besitzer der E-Mail-Domain des Absenders festgelegt.
spfVerdict	Gibt an, ob die SPF-Prüfungen (Sender Policy Framework) bestanden wurden. Weitere Informationen finden Sie unter Inhalt der Benachrichtigungen für den E-Mail-Empfang von Amazon SES im Amazon Simple Email Service Developer Guide.
messageTimestamp	Gibt an, wann die Nachricht empfangen wurde.

`MAILBOX_EMAIL_DELIVERED`

Dieses Ereignis wird protokolliert, wenn eine Nachricht an ein Postfach in Ihrer Organisation zugestellt wird. Dies wird einmal für jedes Postfach protokolliert, an das eine Nachricht geliefert wird. Somit kann ein einzelnes `ORGANIZATION_EMAIL_RECEIVED`-Ereignis zu mehreren `MAILBOX_EMAIL_DELIVERED`-Ereignissen führen.

Feld	Beschreibung
Empfänger	Das Postfach, an das die Nachricht geliefert wird.
folder	Die E-Mail-Ordner, in dem die Nachricht platziert wird.

`RULE_APPLIED`

Dieses Ereignis wird protokolliert, wenn eine eingehende oder ausgehende Nachricht eine E-Mail-Flussregel auslöst.

Feld	Beschreibung
ruleName	Der Name der Regel.
ruleType	Der Typ der angewendeten Regel (INBOUND_RULE, OUTBOUND_RULE oder MAILBOX_RULE). Die Regeln für eingehende und ausgehende Sendungen gelten für Ihre WorkMail Amazon-Organisation. Regeln gelten nur für angegebene E-Mail-Postfächer. Weitere Informationen finden Sie unter E-Mail-Fluss verwalten.
ruleActions	Aufgrund einer Regel durchgeführte Aktionen. Für die einzelnen Empfänger der Nachricht sind möglicherweise verschiedene Aktionen durchgeführt wurden, beispielsweise für unzustellbare E-Mails oder erfolgreich zugestellte.
targetFolder	Vorgesehener Zielordner für eine `Move`- oder `Copy`-MAILBOX_RULE.

Feld	Beschreibung
targetRecipient	Vorgesehener Empfänger für eine `Forward`- oder `Redirect`-MAILBOX_RULE.

`JOURNALING_INITIATED`

Dieses Ereignis wird protokolliert, wenn Amazon eine E-Mail an die vom Administrator Ihrer Organisation angegebene Journal-Adresse WorkMail sendet. Eine Übertragung findet nur statt, wenn die Journal-Erstellung für Ihre Organisation konfiguriert ist. Weitere Informationen finden Sie unter E-Mail-Journaling mit Amazon verwenden WorkMail.

Feld	Beschreibung
journalingAddress	Die E-Mail-Adresse, an die die Journal-Nachricht gesendet wird.

`INCOMING_EMAIL_BOUNCED`

Dieses Ereignis wird protokolliert, wenn eine eingehende Nachricht nicht an einen Zielempfänger zugestellt werden kann. E-Mails können aus einer Reihe von Gründen zurückgeschickt werden, z. B. wenn das Zielpostfach voll ist. Das System protokolliert dieses Ereignis einmal für jeden Empfänger, was zu einer zurückgesendeten E-Mail führt. Beispiel: Wenn eine eingehende Nachricht an drei Empfänger adressiert ist und zwei von diesen volle Postfächer haben, werden zwei INCOMING_EMAIL_BOUNCED-Ereignisse protokolliert.

Feld	Beschreibung
bouncedRecipient	Der beabsichtigte Empfänger, für den Amazon die WorkMail Nachricht zurückgeschickt hat.

`OUTGOING_EMAIL_SUBMITTED`

Dieses Ereignis wird protokolliert, wenn ein Benutzer in Ihrer Organisation eine E-Mail-Nachricht zur Übertragung übermittelt. Dies wird protokolliert, bevor die Nachricht Amazon verlässt. WorkMail Daher gibt dieses Ereignis keinen Hinweis darauf, ob die E-Mail erfolgreich zugestellt wurde.

Feld	Beschreibung
recipients	Der Empfänger der Nachricht, wie er vom Absender angegeben wurde. Enthält alle Empfänger der Zeilen To (An), CC und BCC.
sender	Die E-Mail-Adresse des Benutzers, der die E-Mail-Nachricht im Namen eines anderen Benutzers gesendet hat. Dieses Feld wird nur eingestellt, wenn eine E-Mail im Namen eines anderen Benutzers gesendet wird.
from	Die Adresse für From (Von). Dies ist in der Regel die E-Mail-Adresse des Benutzers, der die Nachricht gesendet hat. Wenn der Benutzer die Nachricht als ein anderer Benutzer oder im Auftrag eines anderen Benutzers gesendet hat, gibt das Feld die E-Mail-Adresse des Benutzers zurück, in dessen Auftrag die E-Mail gesendet wurde, und nicht die E-Mail-Adresse des tatsächlichen Absenders.
subject	Der Betreff der E-Mail-Nachricht.

`OUTGOING_EMAIL_SENT`

Dieses Ereignis wird protokolliert, wenn eine ausgehende E-Mail erfolgreich an einen Ziel Empfänger zugestellt wurde. Dies wird nur einmal pro erfolgreichem Empfänger protokolliert, sodass ein einzelner `OUTGOING_EMAIL_SUBMITTED`-Eintrag zu mehreren `OUTGOING_EMAIL_SENT`-Einträgen führen kann.

Feld	Beschreibung
Empfänger	Der Empfänger der erfolgreich zugestellten E-Mail.

Feld	Beschreibung
sender	Die E-Mail-Adresse des Benutzers, der die E-Mail-Nachricht im Namen eines anderen Benutzers gesendet hat. Dieses Feld wird nur eingestellt, wenn eine E-Mail im Namen eines anderen Benutzers gesendet wird.
from	Die Adresse für From (Von). Dies ist in der Regel die E-Mail-Adresse des Benutzers, der die Nachricht gesendet hat. Wenn der Benutzer die Nachricht als ein anderer Benutzer oder im Auftrag eines anderen Benutzers gesendet hat, gibt das Feld die E-Mail-Adresse des Benutzers zurück, in dessen Auftrag die E-Mail gesendet wurde, und nicht die E-Mail-Adresse des tatsächlichen Absenders.
messageId	Die SMTP-Nachrichten-ID

`OUTGOING_EMAIL_BOUNCED`

Dieses Ereignis wird protokolliert, wenn eine ausgehende Nachricht nicht an einen Zielempfänger zugestellt werden kann. E-Mails können aus einer Reihe von Gründen zurückgeschickt werden, z. B. wenn das Zielpostfach voll ist. Das System protokolliert für jeden Empfänger einen Bounce-Vorgang, der zu einer zurückgesendeten E-Mail führt. Beispiel: Wenn eine ausgehende Nachricht an drei Empfänger adressiert ist und zwei von diesen volle Postfächer haben, werden zwei `OUTGOING_EMAIL_BOUNCED`-Ereignisse protokolliert.

Feld	Beschreibung
bouncedRecipient	Der beabsichtigte Empfänger, an den der Ziel-E-Mail-Server die Nachricht nicht zustellen konnte.

`DMARC_POLICY_APPLIED`

Dieses Ereignis wird protokolliert, wenn eine DMARC-Richtlinie auf eine E-Mail angewendet wird, die an Ihre Organisation gesendet wird.

Feld	Beschreibung
from	Die Adresse für From (Von). Dies ist in der Regel die E-Mail-Adresse des Benutzers, der die Nachricht gesendet hat. Wenn der Benutzer die Nachricht als ein anderer Benutzer oder im Auftrag eines anderen Benutzers gesendet hat, gibt das Feld die E-Mail-Adresse des Benutzers zurück, in dessen Auftrag die E-Mail gesendet wurde, und nicht die E-Mail-Adresse des tatsächlichen Absenders.
recipients	Die beabsichtigten Empfänger der Nachricht.
policy	Die angewandte DMARC-Richtlinie, die die Aktion angibt, die für die E-Mail ausgeführ t werden soll, wenn die DMARC-Prüfung fehlschlägt (NONE, QUARANTINE oder REJECT). Dies ist identisch mit dem dmarcPolicy-Feld im ORGANIZATION_EMAIL _RECEIVED-Ereignis.

Überwachung der WorkMail Amazon-Auditprotokolle

Sie können Auditprotokolle verwenden, um den Zugriff auf die Postfächer Ihrer WorkMail Amazon-Organisation zu überwachen. Amazon WorkMail protokolliert fünf Arten von Prüfereignissen. Diese Ereignisse können in CloudWatch Logs, Amazon S3 oder Amazon Firehouse veröffentlicht werden. Sie können Auditprotokolle verwenden, um Benutzerinteraktionen mit den Postfächern Ihres Unternehmens, Authentifizierungsversuche und die Bewertung von Zugriffskontrollregeln zu überwachen und Aufrufe von Verfügbarkeitsanbietern an externe Systeme durchzuführen und Ereignisse mit persönlichen Zugriffstoken zu überwachen. Informationen zur Konfiguration der Überwachungsprotokollierung finden Sie unterAudit-Protokollierung aktivieren.

In den folgenden Abschnitten werden die von Amazon protokollierten Prüfereignisse WorkMail, der Zeitpunkt der Übertragung der Ereignisse und Informationen zu den Ereignisfeldern beschrieben.

Protokolle des Postfach-Zugriffs

Postfachzugriffsereignisse liefern Informationen darüber, welche Aktion für welches Postfachobjekt ergriffen (oder versucht) wurde. Für jeden Vorgang, den Sie für ein Element oder einen Ordner in einem Postfach ausführen möchten, wird ein Postfachzugriffsereignis generiert. Diese Ereignisse sind nützlich, um den Zugriff auf Postfachdaten zu überwachen.

Feld	Beschreibung
event_timestamp	Wann das Ereignis eingetreten ist, in Milliseku nden seit der Unix-Zeit.
request_id	Die ID, die die Anfrage eindeutig identifiziert.
organization_arn	Der ARN der & WorkMail Amazon-Organisatio n, zu der der authentifizierte Benutzer gehört.
user_id	Die ID des authentifizierten Benutzers.
impersonator_id	Die ID des Imitators. Nur vorhanden, wenn die Identitätswechselfunktion für die Anfrage verwendet wurde.
Protokoll	Das verwendete Protokoll. Das Protokoll kann sein:`AutoDiscover` ,`EWS`,`IMAP`,`WindowsOu tlook` ,`ActiveSyn c` ,`SMTP`,`WebMail`,`IncomingEmail` , oder`OutgoingEmail` .
source_ip	Die Quell-IP-Adresse der Anforderung.
user_agent	Der Benutzeragent, der die Anfrage gestellt hat.
action	Die für das Objekt ausgeführ te Aktion. Dies kann sein: `readread_hierarchy` ,`read_summ ary` ,`read_attachment` ,`read_perm`

Feld	Beschreibung
	issions ,create,update,update_permissions ,update_read_state ,delete,submit_email_for_sending ,abort_sending_email ,move,move_to,copy, odercopy_to.
owner_id	Die ID des Benutzers, dem das Objekt gehört, auf das reagiert wird.
object_type	Der Objekttyp, der sein kann: Ordner, Nachricht oder Anlage.
item_id	Die ID, die die Nachricht eindeutig identifiziert, die der Betreff des Ereignisses ist oder die den Anhang enthält, der den Betreff des Ereignisses darstellt.
folder_path	Der Pfad des Ordners, für den eine Aktion ausgeführt wird, oder der Pfad des Ordners, der das Objekt enthält, auf das reagiert wird.
folder_id	Die ID, die den Ordner eindeutig identifiziert, der Gegenstand des Ereignisses ist oder der das Objekt enthält, das Gegenstand des Ereignisses ist.
attachment_path	Der Pfad der Anzeigenamen zum betroffenen Anhang.
action_allowed	Ob die Aktion erlaubt war. Kann wahr oder falsch sein.

Protokolle zur Zugriffskontrolle

Zugriffskontrollereignisse werden immer dann generiert, wenn eine Zugriffskontrollregel ausgewertet wird. Diese Protokolle sind nützlich, um verbotene Zugriffe zu überprüfen oder Zugriffskontrollkonfigurationen zu debuggen.

Feld	Beschreibung
event_timestamp	Wann das Ereignis eingetreten ist, in Milliseku nden seit der Unix-Epoche.
request_id	Die ID, die die Anfrage eindeutig identifiziert.
organization_arn	Der ARN der WorkMail Organisation, zu der der authentifizierte Benutzer gehört.
user_id	Die ID des authentifizierten Benutzers.
impersonator_id	Die ID des Imitators. Nur vorhanden, wenn die Identitätswechselfunktion für die Anfrage verwendet wurde.
Protokoll	Das verwendete Protokoll, das sein kann:`AutoDiscover` ,,`EWS`,`IMAP`,`WindowsOutlook` ,,`ActiveSync` , `SMTP` `WebMailIncomingEmail` , oder. `OutgoingEmail`
source_ip	Die Quell-IP-Adresse der Anforderung.
scope	Der Geltungsbereich der Regel, der sein kann:`AccessControl` ,`DeviceAccessControl` , oder. `ImpersonationAccessControl`
rule_id	Die ID der übereinstimmenden Zugriffsk ontrollregel. Wenn keine Regeln übereinst immen, ist rule_id nicht verfügbar.

Feld	Beschreibung
access_granted	Ob der Zugriff erlaubt war. Kann wahr oder falsch sein.

Authentifizierungsprotokolle

Authentifizierungsereignisse enthalten Informationen über Authentifizierungsversuche.

> **Note**
>
> Authentifizierungsereignisse werden nicht für Authentifizierungsereignisse über die WorkMail WebMail Amazon-Anwendung generiert.

Feld	Beschreibung
event_timestamp	Wann das Ereignis eingetreten ist, in Milliseku nden seit der Unix-Epoche.
request_id	Die ID, die die Anfrage eindeutig identifiziert.
organization_arn	Der ARN der WorkMail Organisation, zu der der authentifizierte Benutzer gehört.
user_id	Die ID des authentifizierten Benutzers.
user	Der Benutzername, mit dem die Authentif izierung versucht wurde.
Protokoll	Das verwendete Protokoll, das sein kann:`AutoDiscover` ,`EWS`,`IMAP`,`WindowsOu tlook` ,`ActiveSyn c` ,`SMTP`,`WebMail`,`IncomingEmail` , oder`OutgoingEmail` .
source_ip	Die Quell-IP-Adresse der Anforderung.

Feld	Beschreibung
user_agent	Der Benutzeragent, der die Anfrage gestellt hat.
Methode	Die Authentifizierungsmethode. Derzeit wird nur Basic unterstützt.
auth_successful	Ob der Authentifizierungsversuch erfolgreich war. Kann wahr oder falsch sein.
auth_failed_reason	Der Grund für den Authentifizierungsfehler. Nur vorhanden, wenn die Authentifizierung fehlgeschlagen ist.
personal_access_token_id	Die ID des persönlichen Zugriffstokens, das für die Authentifizierung verwendet wird.

Protokolle des persönlichen Zugriffstokens

Für jeden Versuch, ein persönliches Zugriffstoken zu erstellen oder zu löschen, wird ein PAT-Ereignis (Personal Access Token) generiert. Ereignisse mit persönlichen Zugriffstoken geben Aufschluss darüber, ob Benutzer erfolgreich persönliche Zugriffstoken erstellt haben. Die Protokolle für persönliche Zugriffstoken sind nützlich, um Endbenutzer zu überprüfen, die ihre eigenen erstellen und löschen PATs. Bei der Benutzeranmeldung mit persönlichen Zugriffstoken werden Ereignisse in den vorhandenen Authentifizierungsprotokollen generiert. Weitere Informationen finden Sie unter Authentifizierungsprotokolle.

Feld	Beschreibung
event_timestamp	Wann das Ereignis eingetreten ist, in Millisekunden seit der Unix-Epoche.
request_id	Die ID, die die Anfrage eindeutig identifiziert.
organization_arn	Der ARN der WorkMail Organisation, zu der der authentifizierte Benutzer gehört.
user_id	Die ID des authentifizierten Benutzers.

Feld	Beschreibung
user	Der Benutzername des Benutzers, der diese Aktion ausgeführt hat.
Protokoll	Das für die Aktion verwendete Protokoll hat stattgefunden. Dies kann sein: webapp
source_ip	Die Quell-IP-Adresse der Anforderung.
user_agent	Der Benutzeragent, der die Anfrage gestellt hat.
action	Die Aktion des persönlichen Zugriffstokens, die wie folgt lauten kann: erstellen oder löschen.
Name	Der Name des persönlichen Zugriffstokens.
expires_time	Das Datum, an dem das persönliche Zugriffst oken abläuft.
Bereiche	Der Geltungsbereich der Berechtigungen für persönliche Zugriffstoken für das Postfach.

Protokolle des Verfügbarkeitsanbieters

Verfügbarkeitsanbieter-Ereignisse werden für jede Verfügbarkeitsanfrage generiert, die Amazon in Ihrem Namen an Ihren konfigurierten Verfügbarkeitsanbieter WorkMail stellt. Diese Ereignisse sind nützlich, um die Konfiguration Ihres Verfügbarkeitsanbieters zu debuggen.

Feld	Beschreibung
event_timestamp	Wann das Ereignis eingetreten ist, in Milliseku nden seit der Unix-Epoche.
request_id	Die ID, die die Anfrage eindeutig identifiziert.
organization_arn	Der ARN der WorkMail Organisation, zu der der authentifizierte Benutzer gehört.

Feld	Beschreibung
user_id	Die ID des authentifizierten Benutzers.
Typ	Der Typ des aufgerufenen Verfügbarkeitsanbieters. Dies kann sein: `EWS` oder. `LAMBDA`
Domain	Die Domain, für die die Verfügbarkeit erreicht wird.
function_arn	Der ARN des aufgerufenen Lambdas, falls der Typ LAMBDA ist. Andernfalls ist dieses Feld nicht vorhanden.
ews_endpoint	Der Typ des EWS-Endpunkts ist EWS. Andernfalls ist dieses Feld nicht vorhanden.
error_message	Die Meldung, die die Ursache des Fehlers beschreibt. Wenn die Anfrage erfolgreich war, ist dieses Feld nicht vorhanden.
availability_event_successful	Ob die Verfügbarkeitsanfrage erfolgreich bearbeitet wurde.

CloudWatch Insights mit Amazon verwenden WorkMail

Wenn Sie die E-Mail-Ereignisprotokollierung in der WorkMail Amazon-Konsole aktiviert oder die Übermittlung von Auditprotokollen an CloudWatch Logs aktiviert haben, können Sie Amazon CloudWatch Logs Insights verwenden, um Ihre Ereignisprotokolle abzufragen. Weitere Informationen zum Einschalten der E-Mail-Ereignisprotokollierung finden Sie unter Die Protokollierung von E-Mail-Ereignissen aktivieren. Weitere Informationen zu CloudWatch Logs Insights finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im Amazon CloudWatch Logs-Benutzerhandbuch.

Die folgenden Beispiele zeigen, wie CloudWatch Logs nach häufigen E-Mail-Ereignissen abgefragt werden. Sie führen diese Abfragen in der CloudWatch Konsole aus. Anweisungen zur Ausführung dieser Abfragen finden Sie unter Tutorial: Eine Beispielabfrage ausführen und ändern im Amazon CloudWatch Logs-Benutzerhandbuch.

Example Erfahren Sie, warum Benutzer B keine von Benutzer A gesendete E-Mail erhalten hat.

Das folgende Codebeispiel zeigt, wie Sie eine ausgehende E-Mail, die von Benutzer A an Benutzer B gesendet wurde, sortiert nach Zeitstempel abfragen können.

```
fields @timestamp, traceId

| sort @timestamp asc
| filter (event.from like /(?i)userA@example.com/
and event.eventName = "OUTGOING_EMAIL_SUBMITTED"
and event.recipients.0 like /(?i)userB@example.com/)
```

Dies gibt die gesendete Nachricht und Nachverfolgungs-ID zurück. Verwenden Sie die Nachverfolgungs-ID im folgenden Codebeispiel, um die Ereignisprotokolle der gesendeten Nachricht abzufragen.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

Dies gibt die E-Mail-ID und die E-Mail-Ereignisse zurück. `OUTGOING_EMAIL_SENT` gibt an, dass die E-Mail gesendet wurde. `OUTGOING_EMAIL_BOUNCED` weist darauf hin, dass die E-Mail nicht zugestellt wurde. Um zu sehen, ob die E-Mail empfangen wurde, führen Sie eine Abfrage mit der Nachrichten-ID im folgenden Codebeispiel aus.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter event.messageId like "$MESSAGEID"
```

Dies sollte auch die empfangene Nachricht zurückgeben, da diese die gleiche Nachrichten-ID hat. Verwenden Sie die Nachverfolgungs-ID im folgenden Codebeispiel, um die Zustellung abzufragen.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

Dies gibt die Zustellaktion sowie alle zutreffenden Regelaktionen zurück.

Example Sehen Sie sich alle E-Mails an, die von einem Benutzer oder einer Domain empfangen wurden

Das folgende Codebeispiel zeigt, wie Sie alle E-Mails abfragen können, die von einem bestimmten Benutzer empfangen wurden.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like /(?i)user@example.com/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

Das folgende Codebeispiel zeigt, wie Sie alle E-Mails abfragen können, die von einer bestimmten Domäne empfangen wurden.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like "example.com" and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

Example Sehen Sie, wer zurückgesendete E-Mails gesendet hat

Das folgende Codebeispiel zeigt, wie Sie eine Abfrage für ausgehende E-Mails erstellen können, die nicht zugestellt werden konnten. Er liefert zudem auch die Gründe für die Nichtzustellbarkeit.

```
fields @timestamp, event.destination, event.reason
| sort @timestamp desc
| filter event.eventName = "OUTGOING_EMAIL_BOUNCED"
```

Das folgende Codebeispiel zeigt, wie Sie eingehende E-Mails abfragen, die zurückgewiesen wurden. Außerdem werden die E-Mail-Adressen der zurückgesendeten Empfänger und die Gründe für die Zurückweisung zurückgegeben.

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason,
 event.bouncedRecipient.status
| sort @timestamp desc
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

Example Finden Sie heraus, welche Domains Spam versenden

Das folgende Codebeispiel zeigt, wie Sie Empfänger in Ihrer Organisation abfragen können, die Spam erhalten.

```
stats count(*) as c by event.recipients.0
| filter (event.eventName = "ORGANIZATION_EMAIL_RECEIVED" and event.spamVerdict =
 "FAIL")
| sort c desc
```

Das folgende Codebeispiel zeigt, wie Sie die Absender der Spam-E-Mails abfragen können.

```
fields @timestamp, event.recipients.0, event.sender, event.from
| sort @timestamp asc
| filter (event.spamVerdict = "FAIL")
```

Example Erfahren Sie, warum eine E-Mail an den Spam-Ordner eines Empfängers gesendet wurde

Das folgende Codebeispiel zeigt, wie Sie E-Mails, gefiltert nach Betreff, abfragen können, die als Spam identifiziert wurden.

```
fields @timestamp, event.recipients.0, event.spamVerdict, event.spfVerdict,
 event.dkimVerdict, event.dmarcVerdict
| sort @timestamp asc
| filter event.subject like /(?i)$SUBJECT/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED"
```

Sie können auch die Nachverfolgungs-ID der E-Mail abfragen, um alle Ereignisse für die E-Mail einzusehen.

Example Sehen Sie sich E-Mails an, die den E-Mail-Flussregeln entsprechen

Das folgende Codebeispiel zeigt, wie Sie E-Mails abfragen, die mit den E-Mail-Flussregeln für ausgehende Nachrichten übereingestimmt haben.

```
fields @timestamp, event.ruleName, event.ruleActions.0.action
| sort @timestamp desc
| filter event.ruleType = "OUTBOUND_RULE"
```

Das folgende Codebeispiel zeigt, wie Sie E-Mails abfragen, die mit den E-Mail-Flussregeln für eingehende Nachrichten übereingestimmt haben.

```
fields @timestamp, event.ruleName, event.ruleActions.0.action,
 event.ruleActions.0.recipients.0
```

```
| sort @timestamp desc
| filter event.ruleType = "INBOUND_RULE"
```

Example Sehen Sie, wie viele E-Mails von Ihrer Organisation empfangen oder gesendet wurden

Das folgende Codebeispiel zeigt, wie Sie die Anzahl der E-Mails abfragen, die von den einzelnen Empfängern in Ihrer Organisation empfangen wurden.

```
stats count(*) as c by event.recipient
| filter event.eventName = "MAILBOX_EMAIL_DELIVERED"
| sort c desc
```

Das folgende Codebeispiel zeigt, wie Sie die Anzahl der E-Mails abfragen, die von den einzelnen Absendern in Ihrer Organisation gesendet wurden.

```
stats count(*) as c by event.from
| filter event.eventName = "OUTGOING_EMAIL_SUBMITTED"
| sort c desc
```

Protokollierung Amazon WorkMail Amazon-API-Aufrufen mit AWS CloudTrail

Amazon WorkMail ist integriert AWS CloudTrail, ein Service, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS-Service bei Amazon ausgeführt wurden WorkMail. CloudTrail erfasst alle API-Aufrufe für Amazon WorkMail als Ereignisse, einschließlich Aufrufe von der WorkMail Amazon-Konsole und von Codeaufrufen an Amazon WorkMail APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon WorkMail. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Amazon gestellt wurde WorkMail, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

WorkMail Amazon-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in Amazon Aktivitäten auftreten WorkMail, wird diese Aktivität zusammen mit anderen AWS-Service Ereignissen

in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Veranstaltungen für Amazon WorkMail, müssen Sie einen Trail erstellen. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle WorkMail Amazon-Aktionen werden von Amazon protokolliert CloudTrail und sind in der Amazon WorkMail API-Referenz dokumentiert. Beispielsweise werden durch Aufrufe der API-Operationen `CreateUser`, `CreateAlias` und `GetRawMessageContent` Einträge in den CloudTrail-Protokolldateien generiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anforderung mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Service gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

WorkMail Amazon-Protokolldateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis ist eine einzelne Anforderung aus einer beliebigen Quelle und enthält Informationen zur angeforderten Aktion, zu Datum und Uhrzeit der Aktion, zu den Anforderungsparametern usw. CloudTrail -Protokolldateien stellen kein geordnetes Stack-Trace der öffentlichen API-Aufrufe dar. Daher werden sie nicht in einer bestimmten Reihenfolge angezeigt.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateUser` Aktion der WorkMail Amazon-API demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T17:49:59Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "name": "janedoe",
    "displayName": "Jane Doe",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": {
    "userId": "a3a9176d-EXAMPLE"
  },
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateAlias` Aktion der WorkMail Amazon-API demonstriert.


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
    "entityId": "a3a9176d-EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```


Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `GetRawMessageContent` Aktion der Amazon WorkMail Message Flow API demonstriert.


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmailMessageFlow.amazonaws.com",
  "eventName": "GetRawMessageContent",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "messageId": "123A4A5A-67B8-90C1-D23E-45FG67H890J1"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```


Die Protokollierung von E-Mail-Ereignissen aktivieren

Sie aktivieren die Protokollierung von E-Mail-Ereignissen in der WorkMail Amazon-Konsole, um E-Mail-Nachrichten für Ihre Organisation nachzuverfolgen. Die E-Mail-Ereignisprotokollierung verwendet eine AWS Identity and Access Management serviceverknüpfte Rolle (SLR), um Berechtigungen zur Veröffentlichung der E-Mail-Ereignisprotokolle auf Amazon zu erteilen. CloudWatch Weitere Informationen zu serviceverknüpften IAM-Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für Amazon WorkMail

In den CloudWatch Ereignisprotokollen können Sie CloudWatch Suchtools und Messwerte verwenden, um Nachrichten nachzuverfolgen und E-Mail-Probleme zu beheben. Weitere Informationen zu den Ereignisprotokollen, an die Amazon WorkMail sendet CloudWatch, finden Sie unterÜberwachung der WorkMail E-Mail-Ereignisprotokolle von Amazon. Weitere Informationen zu CloudWatch Logs finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Themen

- Einschalten der E-Mail-Ereignisprotokollierung
- Erstellen einer benutzerdefinierten Protokollgruppe und einer IAM-Rolle für die Protokollierung von E-Mail-Ereignissen
- Ausschalten der E-Mail-Ereignisprotokollierung

- Serviceübergreifende Confused-Deputy-Prävention

Einschalten der E-Mail-Ereignisprotokollierung

Folgendes passiert, wenn Sie die E-Mail-Ereignisprotokollierung mit den Standardeinstellungen Amazon aktivieren WorkMail:

- Erstellt eine AWS Identity and Access Management serviceverknüpfte Rolle —`AmazonWorkMailEvents`.
- Erzeugt eine CloudWatch Protokollgruppe —`/aws/workmail/emailevents/`*`organization-alias`*.
- Legt die CloudWatch Protokollspeicherung auf 30 Tage fest.

So schalten Sie E-Mail-Ereignisprotokollierung ein

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich die Option Protokollierungseinstellungen aus.
4. Wählen Sie die Registerkarte Einstellungen für das E-Mail-Flussprotokoll aus.
5. Wählen Sie im Abschnitt Einstellungen für das E-Mail-Flussprotokoll die Option Bearbeiten aus.
6. Stellen Sie den Schieberegler E-Mail-Ereignisse aktivieren auf die Position Ein.
7. Führen Sie eine der folgenden Aktionen aus:

   - (Empfohlen) Wählen Sie „Standardeinstellungen verwenden“.
   - (Optional) Deaktivieren Sie die Option Standardeinstellungen verwenden und wählen Sie eine Zielprotokollgruppe und eine IAM-Rolle aus den angezeigten Listen aus.

     > **Note**
     >
     > Wählen Sie diese Option nur, wenn Sie bereits eine Protokollgruppe und eine benutzerdefinierte IAM-Rolle mit dem erstellt haben. AWS CLI Weitere Informationen

finden Sie unter Erstellen einer benutzerdefinierten Protokollgruppe und einer IAM-Rolle für die Protokollierung von E-Mail-Ereignissen.

8. Wählen Sie Ich autorisiere Amazon WorkMail , mithilfe dieser Konfiguration Protokolle in meinem Konto zu veröffentlichen.
9. Wählen Sie Save (Speichern) aus.

Erstellen einer benutzerdefinierten Protokollgruppe und einer IAM-Rolle für die Protokollierung von E-Mail-Ereignissen

Wir empfehlen, die Standardeinstellungen zu verwenden, wenn Sie die E-Mail-Ereignisprotokollierung für Amazon aktivieren WorkMail. Wenn Sie eine benutzerdefinierte Überwachungskonfiguration benötigen, können Sie die verwenden, AWS CLI um eine dedizierte Protokollgruppe und eine benutzerdefinierte IAM-Rolle für die E-Mail-Ereignisprotokollierung zu erstellen.

Um eine benutzerdefinierte Protokollgruppe und eine IAM-Rolle für die E-Mail-Ereignisprotokollierung zu erstellen

1. Verwenden Sie den folgenden AWS CLI Befehl, um eine Protokollgruppe in derselben AWS Region wie Ihre WorkMail Amazon-Organisation zu erstellen. Weitere Informationen finden Sie unter create-log-group in der Referenz zum AWS CLI -Befehl.

```
aws --region us-east-1 logs create-log-group --log-group-name workmail-monitoring
```

2. Erstellen Sie eine Datei mit der folgenden Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "events.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. Verwenden Sie den folgenden AWS CLI Befehl, um eine IAM-Rolle zu erstellen und diese Datei als Rollenrichtlinien-Dokument anzuhängen. Weitere Informationen finden Sie unter create-role in der AWS CLI -Befehlsreferenz.

```
aws iam create-role --role-name workmail-monitoring-role --assume-role-policy-
document file://trustpolicyforworkmail.json
```

> **Note**
>
> Wenn Sie ein Benutzer mit `WorkMailFullAccess` verwalteten Richtlinien sind, müssen Sie den Begriff `workmail` in den Rollennamen aufnehmen. Diese verwaltete Richtlinie erlaubt Ihnen nur das Konfigurieren der E-Mail-Ereignisprotokollierung zur Verwendung von Rollen, die `workmail` im Namen enthalten. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Gewähren von Benutzerberechtigungen zur AWS Übergabe einer Rolle an einen Dienst.

4. Erstellen Sie eine Datei mit der Richtlinie für die IAM-Rolle, die Sie im vorherigen Schritt erstellt haben. Die Richtlinie muss der Rolle mindestens die Berechtigungen zum Erstellen von Protokoll-Streams und zum Platzieren von Protokollereignissen in der in Schritt 1 erstellten Protokollgruppe gewähren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:111122223333:log-group:workmail-
monitoring*"
        }
    ]
}
```

5. Verwenden Sie den folgenden AWS CLI Befehl, um die Richtliniendatei an die IAM-Rolle anzuhängen. Weitere Informationen finden Sie unter put-role-policy in der Referenz zum AWS CLI -Befehl.

```
aws iam put-role-policy --role-name workmail-monitoring-role --policy-
name workmail-permissions --policy-document file://rolepolicy.json
```

Ausschalten der E-Mail-Ereignisprotokollierung

Schalten Sie die Protokollierung von E-Mail-Ereignissen von der WorkMail Amazon-Konsole aus. Wenn Sie die E-Mail-Ereignisprotokollierung nicht mehr verwenden müssen, empfehlen wir Ihnen, auch die zugehörige CloudWatch Protokollgruppe und die mit dem Dienst verknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle für Amazon WorkMail.

So deaktivieren Sie E-Mail-Ereignisprotokollierung

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Monitoring (Überwachung) aus.
4. Wählen Sie im Abschnitt Protokolleinstellungen die Option Bearbeiten aus.
5. Stellen Sie den Schieberegler E-Mail-Ereignisse aktivieren auf die Position Aus.
6. Wählen Sie Save (Speichern) aus.

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS kann ein dienstübergreifendes Identitätswechsels zum Problem des verwirrten Stellvertreters führen. Ein serviceübergreifender Identitätswechsel kann auftreten, wenn ein Service (der Anruf-Service) einen anderen Service anruft (den aufgerufenen Service).

Der anrufende Service kann so manipuliert werden, dass er seine Berechtigungen nutzt, um auf die Ressourcen eines anderen Kunden zu reagieren, für den er sonst keine Zugriffsberechtigung hätte.

Um dies zu verhindern, werden Tools AWS bereitgestellt, mit denen Sie Ihre Daten für alle Dienste schützen können, deren Dienstprinzipale Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die CloudWatch Logs und Amazon S3 den Services gewähren, die Protokolle generieren. Wenn Sie beide Kontextschlüssel für globale Bedingungen verwenden, müssen die Werte dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienerklärung verwendet werden.

Die Werte von `aws:SourceArn` müssen denen ARNs der Lieferquellen entsprechen, die Protokolle generieren.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (*) für die unbekannten Teile des ARN.

Audit-Protokollierung aktivieren

Sie können Auditprotokolle verwenden, um detaillierte Informationen über die Nutzung Ihrer WorkMail Amazon-Organisation zu erfassen. Die Auditprotokolle können verwendet werden, um den Zugriff von Benutzern auf Postfächer zu überwachen, nach verdächtigen Aktivitäten zu suchen und Konfigurationen von Zugriffskontrollen und Verfügbarkeitsanbietern zu debuggen.

> **Note**
>
> Die AmazonWorkMailFullAccessverwaltete Richtlinie umfasst nicht alle erforderlichen Berechtigungen für die Verwaltung von Protokollzustellungen. Wenn Sie diese Richtlinie zur Verwaltung verwenden WorkMail, stellen Sie sicher, dass der für die Konfiguration der Protokollzustellungen verwendete Prinzipal (z. B. die angenommene Rolle) auch über alle erforderlichen Berechtigungen verfügt.

Amazon WorkMail unterstützt drei Lieferziele für Audit-Logs: CloudWatch Logs, Amazon S3 und Amazon Data Firehose. Weitere Informationen finden Sie unter Protokollierung, für die zusätzliche Berechtigungen erforderlich sind [V2] im Amazon CloudWatch Logs-Benutzerhandbuch.

Zusätzlich zu den unter Protokollierung, für die zusätzliche Berechtigungen erforderlich sind [V2] aufgeführten Berechtigungen WorkMail benötigt Amazon eine zusätzliche Berechtigung, um die Protokollzustellung zu konfigurieren:`workmail:AllowVendedLogDeliveryForResource`.

Eine funktionierende Protokollzustellung besteht aus drei Elementen:

- DeliverySource, ein logisches Objekt, das die Ressource oder Ressourcen darstellt, die die Protokolle senden. Für Amazon WorkMail ist es die WorkMail Amazon-Organisation.
- A DeliveryDestination, ein logisches Objekt, das das tatsächliche Lieferziel darstellt.
- Eine Lieferung, die eine Zustellungsquelle mit einem Lieferziel verbindet.

Um die Protokollzustellung zwischen Amazon WorkMail und einem Ziel zu konfigurieren, können Sie wie folgt vorgehen:

- Erstellen Sie eine Lieferquelle mit PutDeliverySource.
- Erstellen Sie ein Lieferziel mit PutDeliveryDestination.
- Wenn Sie Logs kontoübergreifend versenden, müssen Sie PutDeliveryDestinationPolicyim Zielkonto angeben, dass dem Ziel eine IAM-Richtlinie zugewiesen wird. Diese Richtlinie autorisiert die Erstellung einer Lieferung von der Lieferquelle in Konto A zum Lieferziel in Konto B.
- Erstellen Sie eine Lieferung, indem Sie genau eine Lieferquelle und ein Lieferziel verknüpfen, indem Sie. CreateDelivery

In den folgenden Abschnitten finden Sie Einzelheiten zu den Berechtigungen, über die Sie verfügen müssen, wenn Sie angemeldet sind, um die Protokollzustellung an die einzelnen Zieltypen einzurichten. Diese Berechtigungen können einer IAM-Rolle gewährt werden, mit der Sie angemeldet sind.

> **Important**
>
> Es liegt in Ihrer Verantwortung, Ressourcen für die Protokollzustellung zu entfernen, nachdem Sie die Ressource gelöscht haben, die das Protokoll generiert hat.

Gehen Sie wie folgt vor, um Ressourcen für die Protokollübermittlung zu entfernen, nachdem Sie die Ressource gelöscht haben, die das Protokoll generiert hat.

1. Löschen Sie die Lieferung mithilfe des Vorgangs DeleteDelivery.

2. Löschen Sie die DeliverySourcemithilfe der DeleteDeliverySourceOperation.
3. Wenn das mit dem DeliverySource, was Sie gerade gelöscht haben, DeliveryDestinationverknüpft ist, nur für dieses spezielle DeliverySourceObjekt verwendet wird, können Sie es mithilfe des DeleteDeliveryDestinationsVorgangs entfernen.

Konfiguration der Audit-Protokollierung mit der WorkMail Amazon-Konsole

Sie können die Audit-Protokollierung in der WorkMail Amazon-Konsole konfigurieren:

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie Protokollierungseinstellungen aus.
4. Wählen Sie den Tab Audit-Log-Einstellungen.
5. Konfigurieren Sie mithilfe des entsprechenden Widgets Lieferungen für den erforderlichen Protokolltyp.
6. Wählen Sie Save (Speichern) aus.

An Logs gesendete CloudWatch Protokolle

Benutzerberechtigungen

Um das Senden von Protokollen an CloudWatch Logs zu ermöglichen, müssen Sie mit den folgenden Berechtigungen angemeldet sein.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
```

```
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyCWL",
            "Effect": "Allow",
            "Action": [
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:*"
            ]
        }
        {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
```

```
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

Protokollgruppe und Ressourcenrichtlinie

Die Protokollgruppe, an die die Protokolle gesendet werden, muss über eine Ressourcenrichtlinie verfügen, die bestimmte Berechtigungen enthält. Wenn die Protokollgruppe derzeit keine Ressourcenrichtlinie hat und der Benutzer, der die Protokollierung einrichtet, über die `logs:DescribeLogGroups` Berechtigungen `logs:PutResourcePolicylogs:DescribeResourcePolicies`, und für die Protokollgruppe verfügt, erstellt er AWS automatisch die folgende Richtlinie für diese Gruppe, wenn Sie beginnen, die Protokolle an Logs zu CloudWatch senden.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AWSLogDeliveryWrite20150319",
            "Effect":"Allow",
            "Principal":{
                "Service":[
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Action":[
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource":[
                "arn:aws:logs:region:account-id:log-group:my-log-group:log-stream:*"
            ],
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
```

```
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:*"
                    ]
                }
            }
        }
    ]
}
```

Überlegungen zur Größenbeschränkung der Protokollgruppen-Ressourcenrichtlinie

Diese Dienste müssen jede Protokollgruppe, an die sie Protokolle senden, in der Ressourcenrichtlinie auflisten. CloudWatch Die Ressourcenrichtlinien für Protokolle sind auf 5.120 Zeichen begrenzt. Ein Dienst, der Protokolle an eine große Anzahl von Protokollgruppen sendet, stößt möglicherweise auf dieses Limit.

Um dies zu verringern, überwacht CloudWatch Logs den Umfang der Ressourcenrichtlinien, die von dem Dienst verwendet werden, der Protokolle sendet. Wenn Logs feststellt, dass sich eine Richtlinie der Größenbeschränkung von 5.120 Zeichen nähert, aktiviert CloudWatch `/aws/vendedlogs/*` Logs automatisch die Ressourcenrichtlinie für diesen Dienst. Sie können dann anfangen, Protokollgruppen als Ziele für Protokolle aus diesen Services zu verwenden, deren Namen mit `/aws/vendedlogs/` beginnt.

An Amazon S3 gesendete Protokolle

Benutzerberechtigungen

Um das Senden von Protokollen an Amazon S3 zu aktivieren, müssen Sie mit den folgenden Berechtigungen angemeldet sein.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
```

```
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
          {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
```

```
        }
    ]
}
```

Der S3-Bucket, an den die Protokolle gesendet werden, muss über eine Ressourcenrichtlinie verfügen, die bestimmte Berechtigungen enthält. Wenn der Bucket derzeit keine Ressourcenrichtlinie hat und der Benutzer, der die Protokollierung einrichtet, über die `S3:GetBucketPolicy` und `S3:PutBucketPolicy` -Berechtigungen für den Bucket verfügt, erstellt er AWS automatisch die folgende Richtlinie dafür, wenn Sie beginnen, die Protokolle an Amazon S3 zu senden.

```
{
    "Version":"2012-10-17",
    "Id":"AWSLogDeliveryWrite20150319",
    "Statement":[
        {
            "Sid":"AWSLogDeliveryAclCheck",
            "Effect":"Allow",
            "Principal":{
                "Service":"delivery.logs.amazonaws.com"
            },
            "Action":"s3:GetBucketAcl",
            "Resource":"arn:aws:s3:::my-bucket",
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:delivery-source:*"
                    ]
                }
            }
        },
        {
            "Sid":"AWSLogDeliveryWrite",
            "Effect":"Allow",
            "Principal":{
                "Service":"delivery.logs.amazonaws.com"
            },
            "Action":"s3:PutObject",
            "Resource":"arn:aws:s3:::my-bucket/AWSLogs/account-id/*",
```

```
            "Condition":{
                "StringEquals":{
                    "s3:x-amz-acl":"bucket-owner-full-control",
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:delivery-source:*"
                    ]
                }
            }
        }
    ]
}
```

Geben Sie in der vorherigen Richtlinie für `aws:SourceAccount` die Liste der Konten an, IDs für die Protokolle an diesen Bucket übermittelt werden. Geben Sie für `aws:SourceArn` die Liste ARNs der Ressource, die die Protokolle generiert, im folgenden Formular an`arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`.

Wenn der Bucket über eine Ressourcenrichtlinie verfügt, diese Richtlinie jedoch nicht die in der vorherigen Richtlinie gezeigte Anweisung enthält und der Benutzer, der die Protokollierung einrichtet, über die `S3:PutBucketPolicy` Berechtigungen `S3:GetBucketPolicy` und für den Bucket verfügt, wird diese Anweisung an die Ressourcenrichtlinie des Buckets angehängt.

> **Note**
>
> In einigen Fällen werden möglicherweise `AccessDenied` Fehler angezeigt, AWS CloudTrail wenn die `s3:ListBucket` Berechtigung nicht erteilt wurde. `delivery.logs.amazonaws.com` Um diese Fehler in Ihren CloudTrail Protokollen zu vermeiden, müssen Sie dem die `s3:ListBucket` Erlaubnis erteilen`delivery.logs.amazonaws.com`. Sie müssen auch die `Condition` Parameter angeben, die zusammen mit dem in der vorherigen Bucket-Richtlinie festgelegten `s3:GetBucketAcl` Berechtigungssatz angezeigt werden. Um dies zu vereinfachen, können Sie das Objekt direkt aktualisieren`Statement`, anstatt ein neues `AWSLogDeliveryAclCheck` zu `“Action”: [“s3:GetBucketAcl”, “s3:ListBucket”]` erstellen.

Serverseitige Verschlüsselung im Amazon-S3-Bucket

Sie können die Daten in Ihrem Amazon S3 S3-Bucket schützen, indem Sie entweder die serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) oder die serverseitige Verschlüsselung mit einem in (SSE-KMS) gespeicherten AWS KMS Schlüssel aktivieren. AWS Key Management Service Weitere Informationen finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung.

Wenn Sie SSE-S3 wählen, ist keine zusätzliche Konfiguration erforderlich. Amazon S3 verarbeitet den Verschlüsselungsschlüssel.

> **Warning**
>
> Wenn Sie SSE-KMS wählen, müssen Sie einen vom Kunden verwalteten Schlüssel verwenden, da die Verwendung eines in diesem Szenario nicht unterstützt wird. Von AWS verwalteter Schlüssel Wenn Sie die Verschlüsselung mit einem AWS verwalteten Schlüssel einrichten, werden die Protokolle in einem unlesbaren Format geliefert.

Wenn Sie einen vom Kunden verwalteten AWS KMS Schlüssel verwenden, können Sie den Amazon-Ressourcennamen (ARN) des vom Kunden verwalteten Schlüssels angeben, wenn Sie die Bucket-Verschlüsselung aktivieren. Fügen Sie Folgendes zur Schlüsselrichtlinie für Ihren vom Kunden verwalteten Schlüssel hinzu (nicht zur Bucket-Richtlinie für Ihren S3-Bucket), damit das Konto für die Protokollzustellung in Ihren S3-Bucket schreiben kann.

Wenn Sie SSE-KMS wählen, müssen Sie einen vom Kunden verwalteten Schlüssel verwenden, da die Verwendung eines AWS verwalteten Schlüssels in diesem Szenario nicht unterstützt wird. Wenn Sie einen vom Kunden verwalteten AWS KMS Schlüssel verwenden, können Sie den Amazon-Ressourcennamen (ARN) des vom Kunden verwalteten Schlüssels angeben, wenn Sie die Bucket-Verschlüsselung aktivieren. Fügen Sie Folgendes zur Schlüsselrichtlinie für Ihren vom Kunden verwalteten Schlüssel hinzu (nicht zur Bucket-Richtlinie für Ihren S3-Bucket), damit das Konto für die Protokollzustellung in Ihren S3-Bucket schreiben kann.

```
{
    "Sid":"Allow Logs Delivery to use the key",
    "Effect":"Allow",
    "Principal":{
        "Service":[
            "delivery.logs.amazonaws.com"
        ]
```

```
    },
    "Action":[
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource":"*",
    "Condition":{
        "StringEquals":{
            "aws:SourceAccount":[
                "account-id"
            ]
        },
        "ArnLike":{
            "aws:SourceArn":[
                "arn:aws:logs:region:account-id:delivery-source:*"
            ]
        }
    }
}
```

Geben Sie für `aws:SourceAccount` die Liste der Konten an, IDs für die Protokolle an diesen Bucket gesendet werden. Geben Sie für `aws:SourceArn` die Liste ARNs der Ressource, die die Protokolle generiert, im folgenden Formular an`arn:aws:logs:`*source-region*`:`*source-account-id*`:*`.

An Firehose gesendete Logs

Benutzerberechtigungen

Um das Senden von Protokollen an Firehose zu ermöglichen, müssen Sie mit den folgenden Berechtigungen angemeldet sein.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
```

```
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyFH",
            "Effect": "Allow",
            "Action": [
                "firehose:TagDeliveryStream"
            ],
            "Resource": [
                "arn:aws:firehose:region:account-id:deliverystream/*"
            ]
        },
        {
            "Sid": "CreateServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
```

```
            "Resource": "arn:aws:iam::account-id:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery"
        }
           {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

IAM-Rollen, die für Ressourcenberechtigungen verwendet werden

Da Firehose keine Ressourcenrichtlinien AWS verwendet, verwendet es IAM-Rollen bei der Einrichtung dieser Protokolle, die an Firehose gesendet werden sollen. AWS erstellt eine dienstverknüpfte Rolle mit dem Namen AWSServiceRoleForLogDelivery. Diese dienstbezogene Rolle umfasst die folgenden Berechtigungen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:ListTagsForDeliveryStream"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/LogDeliveryEnabled": "true"
                }
            },
            "Effect": "Allow"
        }
    ]
}
```

Diese dienstbezogene Rolle gewährt Berechtigungen für alle Firehose-Lieferdatenströme, für die das `LogDeliveryEnabled` Tag auf gesetzt ist. `true` AWS weist dieses Tag dem Ziel-Lieferstream zu, wenn Sie die Protokollierung einrichten.

Diese serviceverknüpfte Rolle verfügt auch über eine Vertrauensrichtlinie, die es dem `delivery.logs.amazonaws.com`-Service-Prinzipal erlaubt, die erforderliche serviceverknüpfte Rolle zu übernehmen. Diese Vertrauensrichtlinie lautet wie folgt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Konsolenspezifische Berechtigungen

Wenn Sie die Protokollzustellung über die Konsole statt über die einrichten, benötigen Sie zusätzlich zu den in den APIs vorherigen Abschnitten aufgeführten Berechtigungen auch die folgenden Berechtigungen:

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AllowLogDeliveryActions",
            "Effect":"Allow",
            "Action":[
                "firehose:DescribeDeliveryStream",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource":[
                "arn:aws:logs:region:account-id:log-group:*",
                "arn:aws:firehose:region:account-id:deliverystream/*",
                "arn:aws:s3:::*"
```

```
            ]
        },
        {
            "Sid":"ListAccessForDeliveryDestinations",
            "Effect":"Allow",
            "Action":[
                "logs:DescribeLogGroups",
                "firehose:ListDeliveryStreams",
                "s3:ListAllMyBuckets"
            ],
            "Resource":"*"
        }
    ]
}
```

Konformitätsvalidierung für Amazon WorkMail

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon im WorkMail Rahmen mehrerer AWS Compliance-Programme. Zu diesen gehören SOC, ISO und C5.

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS-Services in Umfang nach Compliance-Programmen. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS Artifact.

Ihre Compliance-Verantwortung bei der Nutzung von Amazon WorkMail hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Umgebungen beschrieben, auf denen auf Sicherheit und Compliance ausgerichtete Basisumgebungen eingerichtet werden. AWS
- AWS Ressourcen zur Einhaltung von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Config— Dieser AWS Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- AWS Security Hub— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen AWS , die Einhaltung der Sicherheitsstandards und bewährten Verfahren der Sicherheitsbranche zu überprüfen.

Resilienz bei Amazon WorkMail

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur WorkMail bietet Amazon mehrere Funktionen, um Ihre Datenstabilität und Backup-Anforderungen zu erfüllen.

Infrastruktursicherheit bei Amazon WorkMail

> **Note**
>
> Amazon hat die Unterstützung für Transport Layer Security (TLS) 1.0 und 1.1 WorkMail eingestellt. Wenn Sie TLS 1.0 oder 1.1 verwenden, müssen Sie die TLS-Version auf 1.2 aktualisieren. Weitere Informationen finden Sie unter TLS 1.2 zur Einführung der minimalen TLS-Protokollebene für alle AWS-API-Endpunkte.

Als verwalteter Service WorkMail ist Amazon durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um WorkMail über das Netzwerk auf Amazon zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Erste Schritte mit Amazon WorkMail

Nachdem Sie das abgeschlossen habenVoraussetzungen, können Sie mit Amazon beginnen WorkMail. Weitere Informationen finden Sie unter Erste Schritte mit Amazon WorkMail.

In den folgenden Abschnitten erfahren Sie mehr über die Migration vorhandener Postfächer zu Amazon WorkMail, die Interoperabilität mit Microsoft Exchange und WorkMail Amazon-Kontingente.

Themen

- Erste Schritte mit Amazon WorkMail
- Zu Amazon migrieren WorkMail
- Interoperabilität zwischen Amazon WorkMail und Microsoft Exchange
- Verfügbarkeitseinstellungen bei Amazon konfigurieren WorkMail
- Konfigurieren der Verfügbarkeitseinstellungen in Microsoft Exchange
- E-Mail-Routing zwischen Microsoft Exchange- und WorkMail Amazon-Benutzern aktivieren
- Aktivieren der E-Mail-Weiterleitung für einen Benutzer
- Konfiguration nach dem Einrichten
- Mail-Client-Konfiguration
- Deaktivierung des Interoperabilitätsmodus und Außerbetriebnahme Ihres Mailservers
- Fehlerbehebung
- WorkMail Amazon-Kontingente

Erste Schritte mit Amazon WorkMail

Egal, ob Sie ein neuer WorkMail Amazon-Nutzer oder ein bestehender Amazon-Nutzer sind WorkSpaces, beginnen Sie mit Amazon, WorkMail indem Sie die folgenden Schritte ausführen.

> **Note**
>
> Erfüllen Sie die Voraussetzungen, bevor Sie beginnen.

Themen

- Schritt 1: Melden Sie sich bei der WorkMail Amazon-Konsole an

- Schritt 2: Richten Sie Ihre WorkMail Amazon-Website ein
- Schritt 3: WorkMail Amazon-Benutzerzugriff einrichten
- Weitere -Quellen

Schritt 1: Melden Sie sich bei der WorkMail Amazon-Konsole an

Sie müssen sich bei der WorkMail Amazon-Konsole anmelden, bevor Sie Benutzer hinzufügen und deren Konten und Postfächer verwalten können.

Um sich bei der WorkMail Amazon-Konsole anzumelden

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.
2. Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen zu Regionen finden Sie unter Regionen und Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Schritt 2: Richten Sie Ihre WorkMail Amazon-Website ein

1. Nachdem Sie sich bei der WorkMail Amazon-Konsole angemeldet haben, richten Sie Ihre Organisation ein und fügen eine Domain hinzu. Wir empfehlen die Verwendung einer dedizierten Domain für Ihre WorkMail Amazon-Organisation. Weitere Informationen erhalten Sie unter Erstellen einer Organisation und Hinzufügen einer Domäne.
2. (Optional) Sie können wählen, ob Sie eine kostenlose Testdomain verwenden möchten, die von Amazon bereitgestellt wird WorkMail. Wenn Sie sich dafür entscheiden, fahren Sie mit Schritt 4 fort.

> **Note**
>
> Testdomänen verwenden dieses Format: *alias* .awsapps.com. Denken Sie dabei daran, dass Sie Testdomänen nur zum Testen verwenden sollten. Verwenden Sie keine Testdomäne für eine Produktionsumgebung. Außerdem müssen Sie mindestens einen aktivierten Benutzer in Ihrer WorkMail Amazon-Organisation haben. Wenn Sie keinen aktivierten Benutzer haben, kann die Domain für die Registrierung und Nutzung durch andere Kunden verfügbar werden.

3. Wenn Sie eine externe Domain verwenden, verifizieren Sie diese Domain, indem Sie Ihrem Domain Name System (DNS) -Dienst die entsprechenden Text- (TXT) - und Mail Exchange (MX) -Einträge hinzufügen. Mit TXT-Einträgen können Sie Notizen in den DNS eingeben. MX-Einträge spezifizieren die Posteingangsserver. Stellen Sie sicher, dass Sie Ihre Domain als Standard für Ihre Organisation festlegen. Weitere Informationen erhalten Sie unter Verifizieren von Domänen und Auswählen der Standarddomäne.
4. Erstellen Sie neue Benutzer oder aktivieren Sie Ihre vorhandenen Verzeichnisbenutzer für Amazon WorkMail. Weitere Informationen finden Sie unter Hinzufügen eines Benutzers.
5. (Optional) Wenn Sie bereits Microsoft Exchange-Postfächer haben, migrieren Sie diese zu Amazon WorkMail. Weitere Informationen finden Sie unter Zu Amazon migrieren WorkMail.

Nachdem Sie Ihre WorkMail Amazon-Website eingerichtet haben, können Sie WorkMail über die URL der Webanwendung auf Amazon zugreifen.

So finden Sie die URL Ihrer WorkMail Amazon-Webanwendung

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie dazu die Liste Region auswählen, die sich rechts neben dem Suchfeld befindet, und wählen Sie dann die gewünschte Region aus. Weitere Informationen finden Sie unter Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.

   Die Seite mit den Organisationseinstellungen wird angezeigt und die URL wird unter Benutzeranmeldung angezeigt. URLs Sie haben dieses Formular: https://*alias*.awsapps.com/mail.

Schritt 3: WorkMail Amazon-Benutzerzugriff einrichten

Wählen Sie aus den folgenden Optionen, um den WorkMail Amazon-Benutzerzugriff einzurichten:

- Richten Sie den Benutzerzugriff mithilfe des Microsoft Outlook-Clients über einen vorhandenen Desktop-Client ein. Weitere Informationen finden Sie unter Microsoft Outlook mit Ihrem WorkMail Amazon-Konto Connect.
- Richten Sie den Benutzerzugriff von einem mobilen Gerät aus ein, z. B. einem Kindle, Android, iPad oder iPhone. Weitere Informationen finden Sie unter Erste Schritte mit einem Mobilgerät.

- Verwenden Sie zum Einrichten des Benutzerzugriffs eine beliebige Client-Software, die mit dem Internet Mail Access Protocol (IMAP) -Protokoll kompatibel ist. Weitere Informationen finden Sie unter IMAP-Clients mit Ihrem WorkMail Amazon-Konto verbinden.

Weitere -Quellen

- Zu Amazon migrieren WorkMail
- Interoperabilität zwischen Amazon WorkMail und Microsoft Exchange
- WorkMail Amazon-Kontingente

Zu Amazon migrieren WorkMail

Sie können WorkMail von Microsoft Exchange, Microsoft Office 365, G Suite Basic (ehemals Google Apps for Work) und anderen Plattformen zu Amazon migrieren, indem Sie mit einem unserer Partner zusammenarbeiten. Weitere Informationen zu unseren Partnern finden Sie unter WorkMail Amazon-Funktionen.

Themen

- Schritt 1: Benutzer in Amazon erstellen oder aktivieren WorkMail
- Schritt 2: Zu Amazon migrieren WorkMail
- Schritt 3: Schließen Sie die Migration zu Amazon ab WorkMail

Schritt 1: Benutzer in Amazon erstellen oder aktivieren WorkMail

Bevor Sie Ihre Benutzer migrieren, müssen Sie diese Benutzer in Amazon hinzufügen WorkMail , um ihr Postfach bereitzustellen. Weitere Informationen finden Sie unter Hinzufügen eines Benutzers.

Schritt 2: Zu Amazon migrieren WorkMail

Sie können mit beliebigen AWS Migrationspartnern zusammenarbeiten, um zu Amazon zu migrieren WorkMail. Informationen zu diesen Anbietern finden Sie unter WorkMailAmazon-Funktionen.

Um Ihre Postfächer zu migrieren, erstellen Sie einen eigenen WorkMail Amazon-Benutzer, der als Migrationsadministrator fungiert. Das folgende Verfahren erteilt diesem Benutzer die Erlaubnis, auf alle Postfächer in Ihrer Organisation zuzugreifen.

So erstellen Sie einen Migrationsadministrator

1. Führen Sie eine der folgenden Aktionen aus:
   - Erstellen Sie in der WorkMail Amazon-Konsole einen neuen Benutzer, der als Migrationsadministrator fungiert. Weitere Informationen finden Sie unter Hinzufügen eines Benutzers.
   - Erstellen Sie in Ihrem Active Directory einen neuen Benutzer, der als Migrationsadministrator fungiert, und aktivieren Sie den Benutzer dann für Amazon WorkMail. Weitere Informationen finden Sie unter Aktivieren von Benutzern.
2. Wählen Sie im Navigationsbereich der WorkMail Amazon-Konsole Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie Organisationseinstellungen, Migration und anschließend Bearbeiten aus.
4. Stellen Sie den Schieberegler „Migration aktiviert“ auf „Ein“.
5. Öffnen Sie den Migrationsadministrator und wählen Sie einen Benutzer aus.
6. Wählen Sie Speichern.

Schritt 3: Schließen Sie die Migration zu Amazon ab WorkMail

Nachdem Sie Ihre E-Mail-Konten zu Amazon migriert haben WorkMail, können Sie Ihre DNS-Einträge überprüfen und Ihre Desktop- und Mobilclients konfigurieren.

Um die Migration zu Amazon abzuschließen WorkMail

1. Stellen Sie sicher, dass alle DNS-Einträge aktualisiert wurden und dass sie auf Amazon verweisen WorkMail. Weitere Informationen zu den erforderlichen DNS-Datensätzen finden Sie unter Hinzufügen einer Domäne.

   > **Note**
   >
   > Die Aktualisierung des DNS-Eintrags kann mehrere Stunden dauern. Wenn während der Änderung an den MX-Datensätzen neue Elemente in einem Quellpostfach ankommen, führen Sie das Migrationstool erneut aus, um neue Elemente nach Abschluss der DNS-Aktualisierung zu migrieren.

2. Weitere Informationen zur Konfiguration Ihrer Desktop- oder Mobilclients für die Nutzung von Amazon WorkMail finden Sie unter Microsoft Outlook mit Ihrem WorkMail Amazon-Konto verbinden im WorkMail Amazon-Benutzerhandbuch.

Interoperabilität zwischen Amazon WorkMail und Microsoft Exchange

Durch die Interoperabilität zwischen Amazon WorkMail und Microsoft Exchange Server können Sie Unterbrechungen für Ihre Benutzer minimieren WorkMail, wenn Sie Postfächer zu Amazon migrieren oder Amazon WorkMail für einen Teil Ihrer Unternehmenspostfächer verwenden.

Diese Interoperabilität ermöglicht es Ihnen, dieselbe Unternehmensdomäne für Postfächer in beiden Umgebungen zu verwenden. Auf diese Weise können Ihre Benutzer Besprechungen mit bidirektionalem Austausch von Informationen über den Status „Frei/Gebucht“ im Kalender planen.

Voraussetzungen

Bevor Sie die Interoperabilität mit Microsoft Exchange aktivieren, führen Sie die folgenden Schritte aus:

- Stellen Sie sicher, dass mindestens ein Benutzer für Amazon aktiviert ist. WorkMail Dies ist erforderlich, um die Verfügbarkeitseinstellungen für Microsoft Exchange zu konfigurieren. Gehen Sie wie unter Aktivieren der E-Mail-Weiterleitung für einen Benutzer beschrieben vor, um einen Benutzer zu aktivieren.
- Set up an Active Directory (AD) Connector. Wenn Sie einen AD Connector mit Ihrem lokalen Verzeichnis einrichten, können Benutzer weiterhin ihre vorhandenen Unternehmensanmeldedaten verwenden. Weitere Informationen finden Sie unter Erstellen eines AD Connector und Integrieren von Amazon WorkMail in Ihr lokales Verzeichnis.
- Richten Sie Ihre WorkMail Amazon-Organisation ein. Erstellen Sie eine WorkMail Amazon-Organisation, die den von Ihnen eingerichteten AD Connector verwendet.
- Fügen Sie Ihre Unternehmensdomänen zu Ihrer WorkMail Amazon-Organisation hinzu und verifizieren Sie sie dann in der WorkMail Amazon-Konsole. Andernfalls werden E-Mails, die an diesen Alias gesendet werden, nicht zugestellt. Weitere Informationen finden Sie unter Arbeiten mit Domänen
- Migrieren Sie Postfächer zu Amazon WorkMail. Ermöglichen Sie Benutzern die Bereitstellung und Migration von Postfächern aus Ihrer lokalen Umgebung zu Amazon. WorkMail Weitere

Informationen finden Sie unter Bestehende Benutzer aktivieren und zu Amazon WorkMail migrieren.

> **Note**
>
> Aktualisieren Sie DNS-Einträge nicht so, dass sie auf Amazon verweisen WorkMail. So wird sichergestellt, dass Microsoft Exchange der primäre Server für eingehende E-Mails bleibt, solange Sie mit beiden Umgebungen parallel arbeiten möchten.

- Stellen Sie sicher, dass die Benutzerprinzipalnamen (UPNs) in Active Directory mit den primären SMTP-Adressen der Benutzer übereinstimmen.

Amazon sendet WorkMail HTTPS-Anfragen an die Exchange Web Services (EWS) -URL auf Microsoft Exchange, um Informationen zu freien/gebuchten Terminen zu erhalten.

Für EWS-basierte Verfügbarkeitsanbieter WorkMail stellt Amazon HTTPS-Anfragen an die Exchange Web Services (EWS) -URL auf Microsoft Exchange, um Informationen zu freien/gebuchten Terminen zu erhalten. Daher gelten die folgenden Voraussetzungen nur für EWS-basierte Verfügbarkeitsanbieter.

- Stellen Sie sicher, dass die entsprechenden Firewall-Einstellungen so eingerichtet sind, dass der Zugriff über das Internet möglich ist. Der Standard-Port für HTTPS-Anforderungen ist 443.
- Amazon WorkMail kann nur dann erfolgreiche HTTPS-Anfragen an die EWS-URL auf Microsoft Exchange stellen, wenn ein von einer gültigen Zertifizierungsstelle (CA) signiertes Zertifikat in Ihrer Microsoft Exchange-Umgebung verfügbar ist. Weitere Informationen finden Sie unter Erstellen einer Exchange Server-Zertifikatsanforderung für eine Zertifizierungsstelle auf der Microsoft Exchange-Dokumentationswebsite.
- Sie müssen die Standardauthentifizierung für EWS in Microsoft Exchange aktivieren. Weitere Informationen finden Sie im Microsoft MVP Award Program-Blog unter Virtual Directories: Exchange 2013.

Hinzufügen von Domänen und Aktivieren von Postfächern

Fügen Sie Ihre Unternehmensdomänen zu Amazon hinzu, WorkMail damit sie in E-Mail-Adressen verwendet werden können. Stellen Sie sicher, dass die zu Amazon hinzugefügten Domains verifiziert WorkMail sind, und ermöglichen Sie dann Benutzern und Gruppen, Postfächer bei Amazon WorkMail bereitzustellen. Ressourcen können im Interoperabilitätsmodus nicht in WorkMail

Amazon aktiviert werden und sollten in Amazon neu erstellt werden, WorkMail nachdem Sie den Interoperabilitätsmodus deaktiviert haben. Sie können Ressourcen jedoch im Interoperabilitätsmodus zum Planen von Meetings verwenden. Ressourcen von Microsoft Exchange werden in Amazon immer auf der Registerkarte „Benutzer“ angezeigt WorkMail.

- Weitere Informationen finden Sie unter Hinzufügen von Domänen, Aktivieren vorhandener Benutzer und Aktivieren einer vorhandenen Gruppe.

> **Note**
>
> Um die Interoperabilität mit Microsoft Exchange sicherzustellen, aktualisieren Sie die DNS-Einträge nicht so, dass sie auf WorkMail Amazon-Einträge verweisen. Microsoft Exchange bleibt der primäre Server für eingehende E-Mails, solange Sie mit beiden Umgebungen parallel arbeiten möchten.

Aktivieren der Interoperabilität

Wenn Sie keine WorkMail Amazon-Organisation erstellt haben, können Sie die öffentliche API verwenden, um eine neue WorkMail Organisation mit aktiviertem Interoperabilitätsmodus zu erstellen.

Wenn Sie bereits eine WorkMail Amazon-Organisation mit einem AD Connector haben, der mit Active Directory verknüpft ist, und Sie auch über Microsoft Exchange verfügen, wenden Sie sich an den AWS-Support, um Support bei der Aktivierung der Microsoft Exchange-Interoperabilität für eine bestehende WorkMail Amazon-Organisation zu erhalten.

Dienstkonten in Microsoft Exchange und Amazon erstellen WorkMail

> **Note**
>
> Das Erstellen eines Dienstkontos in Exchange ist nicht erforderlich, wenn Exchange nicht als Back-End für einen benutzerdefinierten Verfügbarkeitsanbieter verwendet wird.

Um auf free/busy information, create a service account on both Microsoft Exchange and Amazon WorkMail. The Microsoft Exchange service account is any user on Microsoft Exchange that has

access to the calendar free/busy Kalenderinformationen anderer Exchange-Benutzer zuzugreifen. Da Zugriff standardmäßig gewährt wird, werden keine besonderen Berechtigungen benötigt.

In ähnlicher Weise ist das WorkMail Amazon-Servicekonto jeder Benutzer bei Amazon WorkMail , der Zugriff auf kalenderfreie/gebuchte Kalenderinformationen anderer WorkMail Amazon-Benutzer hat. Dieser Zugriff wird ebenfalls standardmäßig gewährt. Sie müssen den WorkMail Amazon-Benutzer in Ihrem lokalen Verzeichnis erstellen und diesen Benutzer dann für Amazon aktivieren WorkMail, um Amazon WorkMail mit AD Connector in Ihr Verzeichnis zu integrieren.

Beschränkungen im Interoperabilitätsmodus

Wenn sich Ihre Organisation im Interoperabilitätsmodus befindet, müssen Sie das Exchange Admin Center verwenden, um alle Benutzer, Gruppen und Ressourcen zu verwalten. Um WorkMail Amazon-Benutzer und -Gruppen zu aktivieren, verwenden Sie die AWS Management Console. Weitere Informationen finden Sie unter Aktivieren vorhandener Benutzer und und Aktivieren einer vorhandenen Gruppe.

Wenn Sie einen Benutzer oder eine Gruppe für Amazon aktivieren WorkMail, können Sie die E-Mail-Adressen oder Aliase dieser Benutzer und Gruppen nicht bearbeiten. Diese müssen ebenfalls über das Exchange Admincenter konfiguriert werden. Amazon WorkMail synchronisiert alle vier Stunden Änderungen in Ihrem Verzeichnis.

Im Interoperabilitätsmodus können in Amazon WorkMail keine Ressourcen erstellt oder aktiviert werden. Alle Ihre Exchange-Ressourcen sind jedoch im WorkMail Amazon-Adressbuch verfügbar und können wie gewohnt für die Planung von Besprechungen verwendet werden.

Verfügbarkeitseinstellungen bei Amazon konfigurieren WorkMail

Konfigurieren Sie die Verfügbarkeitseinstellungen auf Amazon, WorkMail um die Abfrage externer Systeme zu ermöglichen, Kalenderfunktionen anzubieten und free/busy information. Amazon WorkMail supports two modes of obtaining free/busy Kalenderinformationen von einem Remote-System abzurufen:

- Exchange Web Services (EWS) — In dieser Konfiguration fragt Amazon WorkMail mithilfe des EWS-Protokolls einen Exchange-Server oder eine andere WorkMail Organisation nach Verfügbarkeitsinformationen ab. Dies ist die einfachste Konfiguration, setzt jedoch voraus, dass der EWS-Endpunkt des Exchange-Servers über das öffentliche Internet zugänglich ist.
- Custom Availability Provider (CAP) — In dieser Konfiguration kann ein Administrator eine AWS Lambda Lambda-Funktion konfigurieren, um Informationen zur Benutzerverfügbarkeit für eine

bestimmte E-Mail-Domain abzurufen. Abhängig von Ihrer E-Mail-Serverplattform WorkMail bietet die Verwendung von CAP mit Amazon die folgenden Vorteile:

- Holen Sie sich die Benutzerverfügbarkeit über das interne EWS, ohne dafür die Firewall öffnen zu müssen WorkMail.
- Ermitteln Sie die Benutzerverfügbarkeit von Systemen, die nicht Exchange oder EWS sind, wie Google Workspace (früher bekannt als G Suite).

Themen

- Konfigurieren Sie einen EWS-basierten Verfügbarkeitsanbieter
- Konfiguration eines Anbieters für benutzerdefinierte Verfügbarkeit
- Lambda-Funktion eines benutzerdefinierten Verfügbarkeitsanbieters erstellen

Konfigurieren Sie einen EWS-basierten Verfügbarkeitsanbieter

Gehen Sie wie folgt vor, um EWS-basierte Verfügbarkeitseinstellungen auf der Konsole zu konfigurieren:

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie dazu die Liste Region auswählen, die sich rechts neben dem Suchfeld befindet, und wählen Sie dann die gewünschte Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen einer Organisation aus.
3. Wählen Sie im Navigationsbereich Organisationseinstellungen und dann die Registerkarte Interoperabilität aus.
4. Wählen Sie Verfügbarkeitskonfiguration hinzufügen aus, und geben Sie dann die folgenden Informationen ein:

   - Typ — Wählen Sie EWS aus.
   - Domain — Die Domain, für die versucht WorkMail wird, mit dieser Konfiguration Verfügbarkeitsinformationen abzufragen.
   - EWS-URL — Amazon fragt WorkMail diese URL an den EWS-Endpunkt ab. Weitere Informationen finden Sie im Abschnitt Abrufen der EWS-URL in diesem Handbuch.

- Benutzer-E-Mail-Adresse — Die E-Mail-Adresse des Benutzers, der für die Authentifizierung beim EWS-Endpunkt verwendet WorkMail wird.
- Passwort — Das Passwort, das für WorkMail die Authentifizierung beim EWS-Endpunkt verwendet wird.

5. Wählen Sie Speichern.

Die EWS-URL wird abgerufen

Gehen Sie wie folgt vor, um die EWS-URL für Exchange mithilfe von Microsoft Outlook abzurufen:

1. Melden Sie sich in Windows als Benutzer der Exchange-Umgebung in Microsoft Outlook an.
2. Halten Sie die Taste Strg gedrückt und öffnen Sie das Kontextmenü (rechte Maustaste) auf dem Microsoft Outlook-Symbol in der Taskleiste.
3. Wählen Sie E-Mail testen AutoConfiguration.
4. Geben Sie die E-Mail-Adresse und das Passwort des Microsoft Exchange-Benutzers ein und klicken Sie auf Test.
5. Kopieren Sie im Ergebnisfenster den Wert für Availability Service URL.

Um die EWS-URL für den Austausch mithilfe von abzurufen PowerShell, führen Sie an der PowerShell Eingabeaufforderung den folgenden Befehl aus:

```
Get-WebServicesVirtualDirectory |Select name, *url* | fl
```

Um die EWS-URL für Amazon zu erhalten WorkMail, suchen Sie zunächst die EWS-Domain unter WorkMail Amazon-Endpunkte und Kontingente. Geben Sie die EWS-URL ein — `https://"EWS domain"/EWS/Exchange.asmx` und ersetzen Sie „EWS-Domain“ durch Ihre EWS-Domain.

Konfiguration eines Anbieters für benutzerdefinierte Verfügbarkeit

Gehen Sie wie folgt vor, um einen Custom Availability Provider (CAP) zu konfigurieren:

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie dazu die Liste Region auswählen, die sich rechts neben dem Suchfeld befindet, und wählen Sie dann die gewünschte Region aus.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen einer Organisation aus.
3. Wählen Sie im Navigationsbereich Organisationseinstellungen und dann Interoperabilität aus.

4. Wählen Sie Verfügbarkeitskonfiguration hinzufügen und geben Sie dann die folgenden Informationen ein:

   - Typ — Wählen Sie CAP Lambda aus.
   - Domain — Die Domain, für die versucht WorkMail wird, mit dieser Konfiguration Verfügbarkeitsinformationen abzufragen.
   - ARN — Der ARN der Lambda-Funktion, die die Verfügbarkeitsinformationen bereitstellt.

Informationen zum Erstellen einer CAP-Lambda-Funktion finden Sie unterLambda-Funktion eines benutzerdefinierten Verfügbarkeitsanbieters erstellen.

Lambda-Funktion eines benutzerdefinierten Verfügbarkeitsanbieters erstellen

Benutzerdefinierte Verfügbarkeitsanbieter (CAPs) werden mit einem JSON-basierten Anforderungs- und Antwortprotokoll konfiguriert, das in einem klar definierten JSON-Schema geschrieben ist. Eine Lambda-Funktion analysiert die Anfrage und gibt eine gültige Antwort.

Themen

- Anfrage- und Antwortelemente
- Gewähren von -Zugriff
- Beispiel für die WorkMail Verwendung einer CAP-Lambda-Funktion durch Amazon

Anfrage- und Antwortelemente

Anfordern von Elementen

Im Folgenden finden Sie eine Beispielanforderung, die verwendet wird, um eine CAP für einen WorkMail Amazon-Benutzer zu konfigurieren:

```
{
    "requester": {
        "email": "user1@internal.example.com",
        "userName": "user1",
        "organization": "m-0123456789abcdef0123456789abcdef",
        "userId": "S-1-5-18",
        "origin": "127.0.0.1"
```

```
    },
    "mailboxes": [
        "user2@external.example.com",
        "unknown@internal.example.com"
    ],
    "window": {
        "startDate": "2021-05-04T00:00:00.000Z",
        "endDate": "2021-05-06T00:00:00.000Z"
    }
}
```

Eine Anfrage besteht aus drei Abschnitten: Anforderer, Postfächer und Fenster. Diese werden im Folgenden Auftraggeber und in den Window Abschnitten dieses Handbuchs beschrieben. Postfächer

Auftraggeber

Der Abschnitt „Anforderer“ enthält Informationen über den Benutzer, der die ursprüngliche Anfrage an Amazon WorkMail gestellt hat. CAPs Verwenden Sie diese Informationen, um das Verhalten des Anbieters zu ändern. Diese Daten können beispielsweise verwendet werden, um sich als derselbe Benutzer beim Backend-Verfügbarkeitsanbieter auszugeben, oder bestimmte Details können in der Antwort weggelassen werden.

Feld	Beschreibung	Erforderlich
`Email`	Die primäre E-Mail-Adresse des Anfragenden.	Ja
`Username`	Der Benutzername des Anforderers.	Ja
`Organization`	Die Organisations-ID des Anforderers.	Ja
`UserID`	Die ID des Anforderers.	Ja
`Origin`	Die Remote-Adresse der Anfrage.	Nein
`Bearer`	Für die spätere Verwendung reserviert.	Nein

Postfächer

Der Abschnitt Postfächer enthält eine durch Kommas getrennte Liste von E-Mail-Adressen von Benutzern, für die Verfügbarkeitsinformationen angefordert werden.

Window

Der Fensterbereich enthält das Zeitfenster, für das die Verfügbarkeitsinformationen angefordert werden. Beide `startDate` und `endDate` sind in UTC angegeben und gemäß RFC 3339 formatiert. Es wird nicht erwartet, dass Ereignisse gekürzt werden. Mit anderen Worten, wenn ein Ereignis vor dem definierten Ereignis beginnt`StartDate`, wird der ursprüngliche Start verwendet.

Antwortelemente

Amazon WorkMail wartet 25 Sekunden, um eine Antwort von der CAP-Lambda-Funktion zu erhalten. Nach 25 Sekunden geht Amazon davon aus, WorkMail dass die Funktion ausgefallen ist, und generiert in der GetUserAvailability EWS-Antwort Fehler für die zugehörigen Postfächer. Dadurch wird nicht der gesamte GetUserAvailability Vorgang fehlschlagen.

Im Folgenden finden Sie ein Beispiel für eine Antwort aus der Konfiguration, die zu Beginn dieses Abschnitts definiert wurde:

```
{
    "mailboxes": [{
        "mailbox": "user2@external.example.com",
        "events": [{
            "startTime": "2021-05-03T23:00:00.000Z",
            "endTime": "2021-05-04T03:00:00.000Z",
            "busyType": "BUSY"|"FREE"|"TENTATIVE",
            "details": {  // optional
                "subject": "Late meeting",
                "location": "Chime",
                "instanceType": "SINGLE_INSTANCE"|"RECURRING_INSTANCE"|"EXCEPTION",
                "isMeeting": true,
                "isReminderSet": true,
                "isPrivate": false
            }
        }],
        "workingHours": {
            "timezone": {
                "name": "W. Europe Standard Time"
                "bias": 60,
```

```
                "standardTime": {  // optional (not needed for fixed offsets)
                    "offset": 60,
                    "time": "02:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
                "daylightTime": {  // optional (not needed for fixed offsets)
                    "offset": 0,
                    "time": "03:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
            },
            "workingPeriods":[{
                "startMinutes": 480,
                "endMinutes": 1040,
                "days": ["SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"]
            }]
        }
    },{
        "mailbox": "unknown@internal.example.com",
        "error": "MailboxNotFound"
    }]
}
```

Eine Antwort besteht aus einem einzelnen Abschnitt mit Postfächern, der aus einer Liste von Postfächern besteht. Jedes Postfach, für das die Verfügbarkeit erfolgreich sichergestellt wurde, besteht aus drei Abschnitten: Postfach, Ereignisse und Arbeitszeiten. Wenn der Verfügbarkeitsanbieter keine Verfügbarkeitsinformationen für ein Postfach abrufen konnte, besteht der Abschnitt aus zwei Abschnitten: Postfach und Fehler. Diese werden in den folgenden AbschnittenPostfach,,--Ereignisse, Arbeitszeiten ZeitzoneArbeitszeiträume, und in den Fehler Abschnitten dieses Handbuchs beschrieben.

Postfach

Der Postfachbereich ist die E-Mail-Adresse des Benutzers, die sich im Abschnitt Postfächer der Anfrage befindet.

--Ereignisse

Der Abschnitt Ereignisse enthält eine Liste der Ereignisse, die im angeforderten Fenster auftreten. Jedes Ereignis ist mit den folgenden Parametern definiert:

Feld	Beschreibung	Erforderlich
`startTime`	Die Startzeit des Ereignisses in UTC und formatiert gemäß RFC 3339.	Ja
`endTime`	Die Endzeit des Ereignisses in UTC und formatiert gemäß RFC 3339.	Ja
`busyType`	Der Typ des Ereignisses mit hoher Auslastung. Kann `Busy`, `Free` oder `Tentative` sein.	Ja
`details`	Die Einzelheiten der Veranstaltung.	Nein
`details.subject`	Das Thema der Veranstaltung.	Ja
`details.location`	Der Ort der Veranstaltung.	Ja
`details.instanceType`	Der Instanztyp des Ereignisses. Kann `Single_Instance` , `Recurring_Instance` oder `Exception` sein.	Ja
`details.isMeeting`	Ein boolescher Wert, der angibt, ob die Veranstaltung Teilnehmer hat.	Ja
`details.isReminderSet`	Ein boolescher Wert, der angibt, ob für die Veranstal	Ja

Feld	Beschreibung	Erforderlich
	tung eine Erinnerung festgeleg t wurde.	
`details.isPrivate`	Ein boolescher Wert, der angibt, ob das Ereignis auf privat gesetzt ist.	Ja

Arbeitszeiten

Der Abschnitt Arbeitsstunden enthält Informationen zu den Arbeitszeiten des Postfachbesitzers. Er besteht aus zwei Abschnitten: Zeitzone und Arbeitszeiträume.

Zeitzone

Der Unterabschnitt Zeitzone beschreibt die Zeitzone des Postfachbesitzers. Es ist wichtig, dass die Arbeitszeiten des Benutzers korrekt wiedergegeben werden, wenn der Anfragende in einer anderen Zeitzone arbeitet. Der Verfügbarkeitsanbieter muss die Zeitzone explizit beschreiben, anstatt einen Namen zu verwenden. Die Verwendung der standardisierten Zeitzonenbeschreibung trägt dazu bei, Zeitzoneninkongruenzen zu vermeiden.

Feld	Beschreibung	Erforderlich
`name`	Der Name der Zeitzone.	Ja
`bias`	Der Standard-Offset von GMT in Minuten.	Ja
`standardTime`	Der Beginn der Standardzeit für die angegebene Zeitzone.	Nein
`daylightTime`	Der Beginn der Sommerzeit für die angegebene Zeitzone.	Nein

Sie müssen entweder beide `standardTime` und `daylightTime` definieren oder beide weglassen. Die Felder im `daylightTime` Objekt `standardTime` und sind:

Feld	Beschreibung	Zulässige Werte
`offset`	Der Offset im Verhältnis zum Standard-Offset in Minuten.	N/A
`time`	Die Zeit, zu der der Übergang zwischen Normalzeit und Sommerzeit erfolgt, angegeben als`hh:mm:ss`.	N/A
`month`	Der Monat, in dem der Übergang zwischen Normalzeit und Sommerzeit stattfindet.	`JAN`,`FEB`, `MAR`, `APR`, `JUN`, `JUL`, `AUG`, `SEP`, `OCT`, `NOV`, `DEC`
`week`	Die Woche innerhalb des angegebenen Monats, in der der Übergang zwischen Normalzeit und Sommerzeit stattfindet.	`FIRST`, `SECOND`, `THIRD`, `FOURTH`, `LAST`
`dayOfWeek`	Der Tag innerhalb der angegebenen Woche, an dem der Übergang zwischen Normalzeit und Sommerzeit stattfindet.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Arbeitszeiträume

Der Abschnitt WorkingPeriods enthält ein oder mehrere Objekte für die Arbeitsperiode. Jede Periode definiert den Beginn und das Ende des Arbeitstages für einen oder mehrere Tage.

Feld	Beschreibung	Zulässige Werte
`startMinutes`	Der Beginn des Arbeitstages in Minuten ab Mitternacht.	N/A

Feld	Beschreibung	Zulässige Werte
`endMinutes`	Das Ende des Arbeitstages in Minuten ab Mitternacht.	N/A
`days`	Die Tage, für die dieser Zeitraum gilt.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Fehler

Das Fehlerfeld kann beliebige Fehlermeldungen enthalten. In der folgenden Tabelle ist eine Zuordnung von bekannten Codes zu EWS-Fehlercodes aufgeführt. Alle anderen Meldungen werden zugeordnet`ERROR_FREE_BUSY_GENERATION_FAILED`.

Wert	EWS-Fehlercode	
`MailboxNotFound`	`ERROR_MAIL_RECIPIENT_NOT_FOUND`	
`ErrorAvailabilityConfigNotFound`	`ERROR_AVAILABILITY_CONFIG_NOT_FOUND`	
`ErrorServerBusy`	`ERROR_SERVER_BUSY`	
`ErrorTimeoutExpired`	`ERROR_TIMEOUT_EXPIRED`	
`ErrorFreeBusyGenerationFailed`	`ERROR_FREE_BUSY_GENERATION_FAILED`	
`ErrorResponseSchemaValidation`	`ERROR_RESPONSE_SCHEMA_VALIDATION`	

Gewähren von -Zugriff

Führen Sie den folgenden Lambda-Befehl von AWS Command Line Interface (AWS CLI) aus. Dieser Befehl fügt der Lambda-Funktion, die die CAP analysiert, eine Ressourcenrichtlinie hinzu.

Diese Funktion ermöglicht es dem WorkMail Amazon-Verfügbarkeitsservice, Ihre Lambda-Funktion aufzurufen.

```
aws lambda add-permission \
    --region LAMBDA_REGION \
    --function-name CAP_FUNCTION_NAME \
    --statement-id AllowWorkMail \
    --action "lambda:InvokeFunction" \
    --principal availability.workmail.WM_REGION.amazonaws.com \
    --source-account WM_ACCOUNT_ID \
    --source-arn arn:aws:workmail:WM_REGION:WM_ACCOUNT_ID:organization/ORGANIZATION_ID
```

Fügen Sie im Befehl, sofern angegeben, die folgenden Parameter hinzu:

- *LAMBDA_REGION*— Name der Region, in der das CAP Lambda eingesetzt wird. Beispiel, `us-east-1`.
- *CAP_FUNCTION_NAME*— Name der CAP-Lambda-Funktion.

  > **Note**
  >
  > Dies kann der Name, der Alias oder der teilweise oder vollständige ARN der CAP-Lambda-Funktion sein.

- *WM_REGION*— Name der Region, in der die WorkMail Amazon-Organisation die Lambda-Funktion aufruft.

  > **Note**
  >
  > Nur die folgenden Regionen sind für die Verwendung mit CAP verfügbar:
  >
  > - USA Ost (Nord-Virginia)
  > - USA West (Oregon)
  > - Europa (Irland)

- *WM_ACCOUNT_ID*— Die ID des Organisationskontos.
- *ORGANIZATION_ID*— Die ID der Organisation, die das CAP Lambda aufruft. Zum Beispiel Org-ID: m-934ebb9eb57145d0a6cab566ca81a21f.

> **Note**
>
> *LAMBDA_REGIONWM_REGION*und unterscheidet sich nur, wenn regionsübergreifende Anrufe erforderlich sind. Wenn regionsübergreifende Anrufe nicht erforderlich sind, werden sie dieselben sein.

Beispiel für die WorkMail Verwendung einer CAP-Lambda-Funktion durch Amazon

Ein Beispiel dafür, wie Amazon eine CAP-Lambda-Funktion WorkMail verwendet, um einen EWS-Endpunkt abzufragen, finden Sie in dieser AWS Beispielanwendung im Repository Serverless Applications for Amazon WorkMail GitHub .

Konfigurieren der Verfügbarkeitseinstellungen in Microsoft Exchange

Richten Sie in Microsoft Exchange einen Verfügbarkeitsadressraum ein WorkMail, um alle Anfragen nach Informationen zu freien/gebuchten Kalenderinformationen für aktivierte Benutzer an Amazon weiterzuleiten.

Verwenden Sie den folgenden PowerShell Befehl, um den Adressraum zu erstellen:

```
$credentials = Get-Credential
```

Geben Sie an der Eingabeaufforderung die Anmeldeinformationen des WorkMail Amazon-Servicekontos ein. Der Benutzername sollte eingegeben werden als **`domain\username`** (das heißt,***`orgname`*`.awsapps.com\workmail_service_account_`*`username`***. ***`orgname`***Steht hier für den Namen der WorkMail Amazon-Organisation. Weitere Informationen finden Sie unter Dienstkonten in Microsoft Exchange und Amazon erstellen WorkMail.

```
Add-AvailabilityAddressSpace -ForestName orgname.awsapps.com -AccessMethod OrgWideFB -
Credentials $credentials
```

Weitere Informationen finden Sie unter Hinzufügen in AvailabilityAddressSpace Microsoft Docs.

E-Mail-Routing zwischen Microsoft Exchange- und WorkMail Amazon-Benutzern aktivieren

Mit E-Mail-Routing zwischen Microsoft Exchange Server und Amazon können Benutzer ihre vorhandenen E-Mail-Adressen behalten WorkMail, nachdem sie zu Amazon migriert haben WorkMail. Mit E-Mail-Routing können Sie Microsoft Exchange Server als primären SMTP-Server (Simple Mail Transfer Protocol) für eingehende E-Mails in Ihrer Organisation beibehalten.

Bevor Sie E-Mail-Routing verwenden können, müssen Sie die folgenden Voraussetzungen erfüllen:

- Aktivieren Sie den Interoperabilitätsmodus für Ihre Organisation. Weitere Informationen finden Sie unter Aktivieren der Interoperabilität.
- Stellen Sie sicher, dass Sie Ihre Domain in der WorkMail Amazon-Konsole sehen.
- Stellen Sie sicher, dass unser Microsoft Exchange Server E-Mails an das Internet senden kann. Möglicherweise müssen Sie einen Sendeconnector konfigurieren. Weitere Informationen zu Sendeconnectors finden Sie in der Microsoft-Dokumentation unter Erstellen eines Sendeconnectors in Exchange Server zum Senden von E-Mails an das Internet.

Aktivieren der E-Mail-Weiterleitung für einen Benutzer

Wir empfehlen, dass Sie zuerst die folgenden Schritte für Testbenutzer ausführen, bevor Sie Änderungen an Ihrer Organisation vornehmen.

1. Aktivieren Sie das Benutzerkonto, das Sie zu Amazon WorkMail migrieren. Weitere Informationen finden Sie unter Aktivieren vorhandener Benutzer.
2. Stellen Sie in der WorkMail Amazon-Konsole sicher, dass dem aktivierten Benutzer mindestens zwei E-Mail-Adressen zugeordnet sind.
   - <*workmailuser*@ *orgname* .awsapps.com> (dies wird automatisch hinzugefügt und kann für Tests ohne Ihren Microsoft Exchange verwendet werden.)
   - <*workmailuser*@ *yourdomain* .com> (dies wird automatisch hinzugefügt und ist die primäre Microsoft Exchange-Adresse.)

     Weitere Informationen finden Sie unter Bearbeiten von E-Mail-Benutzer-Adressen.
3. Stellen Sie sicher, dass Sie alle Daten aus dem Postfach in Microsoft Exchange in das Postfach in Amazon migrieren WorkMail. Weitere Informationen finden Sie unter Migration zu Amazon WorkMail.

4. Nachdem alle Daten migriert wurden, deaktivieren Sie das Postfach für den Benutzer auf Microsoft Exchange. Erstellen Sie dann einen E-Mail-Benutzer (oder E-Mail-fähigen Benutzer), dessen externe SMTP-Adresse auf Amazon verweist. WorkMail Verwenden Sie dazu die folgenden Befehle in der Exchange-Verwaltungsshell:

   > **Important**
   >
   > Mit den folgenden Schritten wird der Inhalt des Postfachs gelöscht. Stellen Sie sicher, dass Ihre Daten zu Amazon migriert wurden, WorkMail bevor Sie versuchen, das E-Mail-Routing zu aktivieren. Einige E-Mail-Clients wechseln nicht nahtlos zu Amazon, WorkMail wenn Sie diesen Befehl ausführen. Weitere Informationen finden Sie unter Mail-Client-Konfiguration.

   ```
   $old_mailbox = Get-Mailbox exchangeuser
   ```

   ```
   Disable-Mailbox $old_mailbox
   ```

   ```
   $new_mailuser = Enable-MailUser $old_mailbox.Identity -
   ExternalEmailAddress workmailuser@orgname.awsapps.com -PrimarySmtpAddress
    $old_mailbox.PrimarySmtpAddress
   ```

   ```
   Set-MailUser $new_mailuser -EmailAddresses $old_mailbox.EmailAddresses -
   HiddenFromAddressListsEnabled $old_mailbox.HiddenFromAddressListsEnabled
   ```

   Steht in den obigen Befehlen *orgname* für den Namen Ihrer WorkMail Amazon-Organisation. Weitere Informationen finden Sie unter Postfach deaktivieren und E-Mail-Benutzer aktivieren auf Microsoft TechNet.

5. Senden Sie eine Test-E-Mail an den Benutzer (im obigen Beispiel**workmailuser@yourdomain.com**). Wenn das E-Mail-Routing korrekt aktiviert wurde, sollte sich der Benutzer in sein WorkMail Amazon-Postfach einloggen und die E-Mail erhalten können.

> **Note**
>
> Microsoft Exchange bleibt der primäre Server für eingehende E-Mails, solange Sie mit beiden Umgebungen parallel arbeiten möchten. Um die Interoperabilität mit Microsoft Exchange sicherzustellen, sollten die DNS-Einträge WorkMail erst später aktualisiert werden, sodass sie auf Amazon verweisen.

Konfiguration nach dem Einrichten

Mit den oben genannten Schritten wird ein Benutzerpostfach von Microsoft Exchange Server nach Amazon verschoben WorkMail, während der Benutzer in Microsoft Exchange als Kontakt beibehalten wird. Da der migrierte Benutzer jetzt ein externer E-Mail-Benutzer ist, gelten für Microsoft Exchange Server zusätzliche Einschränkungen. Möglicherweise sind auch zusätzliche Konfigurationsanforderungen erforderlich, um die Migration abzuschließen.

- Der Benutzer kann möglicherweise nicht standardmäßig E-Mails an Gruppen senden. Um diese Funktion zu aktivieren, müssen Sie den Benutzer zu einer Liste sicherer Absender für alle Gruppen hinzufügen. Weitere Informationen finden Sie unter Delivery Management auf Microsoft TechNet.
- Der Benutzer kann möglicherweise keine Ressourcen buchen. Um diese Funktion zu aktivieren, müssen Sie die `ProcessExternalMeetingMessages` Anzahl aller Ressourcen festlegen, auf die der Benutzer zugreifen muss. Weitere Informationen finden Sie unter Set- CalendarProcessing on Microsoft TechNet.

Mail-Client-Konfiguration

Einige E-Mail-Clients wechseln nicht nahtlos zu Amazon WorkMail. Bei diesen Clients muss der Benutzer zusätzliche Einrichtungsschritte ausführen. Je nach E-Mail-Client sind hier unterschiedliche Schritte erforderlich.

- Microsoft Outlook unter Windows — Outlook muss neu gestartet werden. Beim Start müssen Sie festlegen, ob Sie das alte Postfach behalten oder ein temporäres Postfach verwenden möchten. Wählen Sie die Option „Temporäres Postfach“. Konfigurieren Sie anschließend das Microsoft Exchange-Postfach neu.

- Microsoft Outlook auf macOS — Wenn Outlook neu gestartet wird, wird die folgende Meldung angezeigt: Outlook wurde auf den Server ***orgname*** .awsapps.com umgeleitet. Möchten Sie, dass dieser Server Ihre Einstellungen konfiguriert? Akzeptieren Sie den Vorschlag.
- Mail auf iOS — Die Mail-App empfängt keine E-Mails mehr und generiert die Fehlermeldung „E-Mail kann nicht abgerufen werden“. Erstellen Sie das Microsoft Exchange-Postfach neu und konfigurieren Sie es neu.

Deaktivierung des Interoperabilitätsmodus und Außerbetriebnahme Ihres Mailservers

Nachdem Sie Ihre Microsoft Exchange-Postfächer für Amazon konfiguriert haben WorkMail, können Sie den Interoperabilitätsmodus deaktivieren. Wenn Sie keine Benutzer oder Datensätze migriert haben, hat die Deaktivierung des Interoperabilitätsmodus keine Auswirkungen auf Ihre Konfigurationen.

> **Warning**
>
> Bevor Sie den Interoperabilitätsmodus deaktivieren, stellen Sie sicher, dass Sie alle erforderlichen Schritte ausgeführt haben. Wenn Sie dies nicht tun, kann es zu zurückgesendeten E-Mails oder unbeabsichtigtem Verhalten kommen. Wenn Sie die Migration noch nicht abgeschlossen haben, kann das Deaktivieren der Interoperabilität die Abläufe in Ihrer Organisation unterbrechen. Dieser Vorgang kann nicht rückgängig gemacht werden.

Um die Unterstützung des Interoperabilitätsmodus zu deaktivieren

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann die Organisation aus, für die Sie den Interoperabilitätsmodus deaktivieren möchten.
3. Wählen Sie unter Organisationseinstellungen die Option Interoperabilitätsmodus deaktivieren aus.

4. Geben Sie im Dialogfeld Interoperabilitätsmodus deaktivieren den Namen der Organisation ein und wählen Sie Interoperabilitätsmodus deaktivieren aus.

Nach der Deaktivierung der Interoperabilitätsunterstützung werden Benutzer und Gruppen, die nicht für Amazon aktiviert WorkMail sind, aus dem Adressbuch entfernt. Sie können weiterhin alle fehlenden Benutzer oder Gruppen über die WorkMail Amazon-Konsole aktivieren, und sie werden dem Adressbuch hinzugefügt. Ressourcen von Microsoft Exchange können nicht aktiviert werden und werden erst im Adressbuch angezeigt, wenn Sie den folgenden Schritt abgeschlossen haben.

- Ressourcen in Amazon erstellen WorkMail — Sie können Ressourcen in Amazon erstellen WorkMail und dann Delegierte und Buchungsoptionen für diese Ressourcen konfigurieren. Weitere Informationen finden Sie unter Arbeiten mit Ressourcen.
- Einen AutoDiscover DNS-Eintrag erstellen — Konfigurieren Sie einen AutoDiscover DNS-Eintrag für alle E-Mail-Domains in der Organisation. Auf diese Weise können Benutzer von ihren Microsoft Outlook- und mobilen Clients aus eine Verbindung zu ihren WorkMail Amazon-Postfächern herstellen. Weitere Informationen finden Sie unter Verwendung AutoDiscover zur Konfiguration von Endpunkten.
- Wechseln Sie Ihren MX-DNS-Eintrag zu Amazon WorkMail — Um alle eingehenden E-Mails an Amazon zuzustellen WorkMail, müssen Sie Ihren MX-DNS-Eintrag auf Amazon umstellen WorkMail. Es kann bis zu 72 Stunden dauern, bis Änderungen an DNS-Einträgen auf alle DNS-Server übertragen werden.
- Außerbetriebnahme Ihres Mailservers — Nachdem Sie sich vergewissert haben, dass alle E-Mails direkt an Amazon weitergeleitet werden WorkMail, können Sie Ihren Mailserver außer Betrieb nehmen, falls Sie ihn in Zukunft nicht mehr verwenden möchten.

Fehlerbehebung

Lösungen für die am häufigsten auftretenden WorkMail Interoperabilitäts- und Migrationsfehler von Amazon sind unten aufgeführt.

Die URL der Exchange Web Services (EWS) ist ungültig oder nicht erreichbar — Vergewissern Sie sich, dass Sie die richtige EWS-URL haben. Weitere Informationen finden Sie unter Verfügbarkeitseinstellungen bei Amazon konfigurieren WorkMail.

Verbindungsfehler bei der EWS-Validierung — Dies ist ein allgemeiner Fehler und kann folgende Ursachen haben:

- Keine Internetverbindung in Microsoft Exchange.
- Ihre Firewall ist nicht so konfiguriert, dass sie den Zugriff über das Internet zulässt. Stellen Sie sicher, dass Port 443 (der Standardport für HTTPS-Anforderungen) offen ist.

Wenn Sie die Internetverbindungs- und Firewall-Einstellungen bestätigt haben, der Fehler jedoch weiterhin besteht, wenden Sie sich an den AWS-Support.

Ungültiger Benutzername und Passwort bei der Konfiguration der Microsoft Exchange-Interoperabilität — Dies ist ein allgemeiner Fehler und kann folgende Ursachen haben:

- Der Benutzername liegt nicht im erwarteten Format vor. Verwenden Sie das folgende Muster:

```
DOMAIN\username
```

- Ihr Microsoft Exchange-Server ist nicht für grundlegende Authentifizierung für EWS konfiguriert. Weitere Informationen finden Sie im Microsoft MVP Award Program-Blog unter Virtual Directories: Exchange 2013.

Der Benutzer erhält E-Mails mit dem Anhang winmail.dat — Dies kann passieren, wenn verschlüsselte S/MIME-E-Mails von Exchange an Amazon gesendet WorkMail und in Outlook 2016 für Mac oder einem IMAP-Client empfangen werden. Die Lösung besteht darin, den folgenden Befehl in der Exchange-Verwaltungsshell auszuführen.

Set-RemoteDomain -Identity "Default" -TNEFEnabled $false

Wenn Sie die obigen Punkte überprüft haben, der Fehler jedoch weiterhin auftritt, wenden Sie sich an den AWS Support.

WorkMail Amazon-Kontingente

Amazon WorkMail kann sowohl von Unternehmenskunden als auch von Kleinunternehmern genutzt werden. Obwohl wir die meisten Anwendungsfälle unterstützen, ohne dass Änderungen an den Kontingenten vorgenommen werden müssen, schützen wir unsere Benutzer und das Internet vor dem Missbrauch des Produkts. Daher kann es vorkommen, dass einige Kunden auf von uns festgelegte Kontingente stoßen. Dieser Abschnitt beschreibt diese Kontingente und die entsprechenden Änderungsmöglichkeiten.

Einige Kontingentwerte können geändert werden, und bei anderen handelt es sich um feste Kontingente, die nicht geändert werden können. Weitere Informationen zum Anfordern einer Kontingenterhöhung finden Sie unter AWS -Servicekontingente im Allgemeine Amazon Web Services-Referenz.

WorkMail Amazon-Organisations- und Benutzerkontingente

Sie können Ihrer WorkMail Amazon-Organisation bis zu 25 Benutzer für eine kostenlose 30-Tage-Testversion hinzufügen. Nach Ablauf dieses Zeitraums werden Ihnen alle aktiven Benutzer in Rechnung gestellt, sofern Sie sie nicht entfernen oder Ihr WorkMail Amazon-Konto schließen.

In die Berechnung dieser Kontingente fließen alle Nachrichten ein, die an einen anderen Benutzer gesendet werden. Dazu gehören E-Mails, Besprechungsanfragen, Besprechungsantworten, Aufgabenanfragen und Nachrichten, die als Ergebnis einer Regel automatisch weitergeleitet oder umgeleitet werden.

> **Note**
>
> Wenn Sie eine Erhöhung des Kontingents für eine bestimmte Organisation beantragen, müssen Sie den Namen der Organisation in Ihrer Anfrage angeben.

Ressource	Standardkontingent	Obergrenze für Änderungsanfragen
WorkMail Amazon-Organisationen pro AWS Konto	100	Kann je nach Verzeichnistyp einer Organisation erhöht werden. In der AWS Directory Service Konsole können Sie AWS Directory Service Kontingente einsehen und Erhöhungen beantragen. Weitere Informationen finden Sie unter Servicekontingente im Allgemeine AWS-Referenz.

Ressource	Standardkontingent	Obergrenze für Änderungsanfragen
Benutzer pro WorkMail Amazon-Organisation	1.000	Kann je nach Verzeichnistyp der Organisation wie folgt erhöht werden: • WorkMail Amazon-Verzeichnis: bis zu 10 Millionen Benutzer • Simple AD oder AD Connector, groß: bis zu 5.000 Benutzer*. • Simple AD oder AD Connector, klein: bis zu 500 Benutzer*. • Microsoft AD, gehostet von AWS Directory Service: bis zu 10 Millionen Benutzern, abhängig von Ihrer Einrichtung und Konfiguration, *Wenn Sie Simple AD oder AD Connector verwenden, finden Sie weitere Informationen unter AWS Directory Service.
Kostenlose Testbenutzer	Bis zu 25 Benutzer in den ersten 30 Tagen	Der kostenlose Testzeitraum gilt nur für die ersten 25 Benutzer in jeder Organisation. Zusätzliche Benutzer sind nicht im kostenlosen Testangebot enthalten.

Ressource	Standardkontingent	Obergrenze für Änderungsanfragen
Adressierte Empfänger pro AWS Konto und Tag	100.000 Empfänger außerhalb der Organisation, ohne feste Kontingente der Empfänger innerhalb der Organisation.	Es gibt keine Obergrenze. Amazon WorkMail ist jedoch ein geschäftlicher E-Mail-Dienst und nicht für Massen-E-Mail-Dienste vorgesehen. Nutzen Sie für den Massen-E-Mail-Versand Amazon SES oder Amazon Pinpoint.
Empfänger, die pro AWS Konto und Tag unter Verwendung einer der Testdomänen adressiert werden	200 Empfänger, unabhängig vom Ziel	Die Test-Mail-Domain ist nicht für die langfristige Nutzung vorgesehen. Wir empfehlen, dass Sie Ihre eigene Domain hinzufügen und diese als Standarddomain verwenden.

Kontingente für Gruppen werden durch das zugrunde liegende Verzeichnis festgelegt.

WorkMail Organisation, die Quoten festlegt

Ressource	Standardkontingent
Anzahl der Domains pro WorkMail Amazon-Organisation	1.000 Dies ist ein festes Kontingent und kann nicht geändert werden.
Anzahl der Absendermuster in Regeln für den E-Mail-Verkehr pro Regel	250 Dies ist eine feste Quote und kann nicht geändert werden.
Anzahl der Absendermuster in Regeln für den E-Mail-Ablauf pro Organisation	1.000

Ressource	Standardkontingent
	Dies ist eine feste Quote und kann nicht geändert werden.

Kontingente pro Benutzer

In die Berechnung dieser Kontingente fließen alle Nachrichten ein, die an einen anderen Benutzer gesendet werden. Dazu gehören E-Mails, Besprechungsanfragen, Besprechungsantworten, Aufgabenanfragen und Nachrichten, die als Ergebnis einer Regel automatisch weitergeleitet oder umgeleitet werden.

Ressource	Standardkontingent	Oberes Kontingent für Änderungsanfragen
Maximale Größe des Postfachs	50 GB Dies ist eine feste Quote und kann nicht geändert werden.	Nicht zutreffend
Maximale Anzahl von Aliasen pro Benutzer	100 Dies ist eine feste Quote und kann nicht geändert werden.	Nicht zutreffend
Adressierte Empfänger, die pro Benutzer und Tag über die eigene Domäne angesprochen werden.	10.000 Empfänger außerhalb der Organisation, ohne feste Kontingente der Empfänger innerhalb der Organisation.	Es gibt keine Obergrenze. Amazon WorkMail ist jedoch ein geschäftlicher E-Mail-Dienst und nicht für Massen-E-Mail-Dienste vorgesehen. Nutzen Sie für den Massen-E-Mail-Versand Amazon SES oder Amazon Pinpoint.

Nachrichtenkontingente

In die Berechnung dieser Kontingente fließen alle Nachrichten ein, die an einen anderen Benutzer gesendet werden. Dazu gehören E-Mails, Besprechungsanfragen, Besprechungsantworten, Aufgabenanfragen und Nachrichten, die als Ergebnis einer Regel automatisch weitergeleitet oder umgeleitet werden.

Ressource	Standardkontingent
Maximale Größe der eingehenden Nachricht	29 MB unverschlüsselter Daten. Nachrichten werden in einem MIME-Form at empfangen. Die maximale Größe der eingehenden MIME-Nachricht beträgt 40 MB. Dies ist ein festes Kontingent und kann nicht geändert werden.
Maximale Größe der ausgehenden Nachricht	29 MB unverschlüsselter Daten. Nachrichten werden in einem MIME-Format gesendet. Die maximale Größe ausgehender MIME-Nachrichten beträgt 40 MB. Dies ist ein festes Kontingent und kann nicht geändert werden.
Maximale Anzahl von Empfängern pro Nachricht	500 Dies ist eine feste Quote und kann nicht geändert werden.
Maximale Anzahl von Anhängen pro Nachricht	500 Dies ist ein festes Kontingent und kann nicht geändert werden.

Arbeiten mit Organisationen

Bei Amazon WorkMail repräsentiert Ihre Organisation die Benutzer in Ihrem Unternehmen. In der WorkMail Amazon-Konsole sehen Sie eine Liste Ihrer verfügbaren Organisationen. Wenn Ihnen keine zur Verfügung steht, müssen Sie eine Organisation erstellen, um Amazon nutzen zu können WorkMail.

Themen

- Erstellen einer Organisation
- Löschen einer Organisation
- Eine E-Mail-Adresse finden
- Mit Organisationseinstellungen arbeiten
- Markieren einer Organisation
- Arbeiten mit Zugriffssteuerungsregeln
- Festlegen von Postfachaufbewahrungsrichtlinien

Erstellen einer Organisation

Um Amazon nutzen zu können WorkMail, müssen Sie zunächst eine Organisation erstellen. Ein AWS Konto kann mehrere WorkMail Amazon-Organisationen haben. Wenn Sie eine Organisation erstellen, wählen Sie auch eine Domain für die Organisation aus und richten Benutzerverzeichnis und Verschlüsselungseinstellungen ein.

Sie können ein neues Benutzerverzeichnis erstellen oder Amazon in ein WorkMail vorhandenes Verzeichnis integrieren. Sie können Amazon WorkMail mit einem lokalen Microsoft Active Directory, AWS Managed Active Directory oder Simple AD verwenden. Durch die Integration in Ihr lokales Verzeichnis können Sie Ihre vorhandenen Benutzer und Gruppen in Amazon verwenden WorkMail und Benutzer können sich mit ihren vorhandenen Anmeldeinformationen anmelden. Wenn Sie ein lokales Verzeichnis verwenden, müssen Sie zuerst einen AD Connector in AWS Directory Service einrichten. Der AD Connector synchronisiert Ihre Benutzer und Gruppen mit dem WorkMail Amazon-Adressbuch und führt Benutzerauthentifizierungsanfragen durch. Weitere Informationen finden Sie unter Active Directory Connector im AWS Directory Service Administratorhandbuch.

Sie haben auch die Möglichkeit AWS KMS key , eine auszuwählen, die Amazon zur Verschlüsselung des Postfachinhalts WorkMail verwendet. Sie können entweder den standardmäßigen AWS

verwalteten Hauptschlüssel für Amazon WorkMail auswählen oder einen vorhandenen KMS-Schlüssel in AWS Key Management Service (AWS KMS) verwenden. Informationen zum Erstellen eines neuen KMS-Schlüssels finden Sie unter Creating Keys im AWS Key Management Service Developer Guide. Wenn Sie als AWS Identity and Access Management (IAM-) Benutzer angemeldet sind, machen Sie sich selbst zum Schlüsseladministrator für den KMS-Schlüssel. Weitere Informationen finden Sie unter Schlüssel aktivieren und deaktivieren im AWS Key Management Service Entwicklerhandbuch.

Überlegungen

Denken Sie beim Erstellen einer WorkMail Amazon-Organisation an Folgendes:

- Amazon unterstützt derzeit WorkMail keine verwalteten Microsoft Active Directory-Dienste, die Sie mit mehreren Konten gemeinsam nutzen.
- Wenn Sie über ein lokales Active Directory mit Microsoft Exchange und einem AD Connector verfügen, empfehlen wir, die Interoperabilitätseinstellungen für Ihre Organisation zu konfigurieren. Auf diese Weise können Sie Unterbrechungen für Ihre Benutzer minimieren WorkMail, wenn Sie Postfächer zu Amazon migrieren oder Amazon WorkMail für einen Teil Ihrer Unternehmenspostfächer verwenden. Weitere Informationen finden Sie unter Interoperabilität zwischen Amazon WorkMail und Microsoft Exchange.
- Wenn Sie die Option Kostenlose Testdomain auswählen, können Sie beginnen, Ihre WorkMail Amazon-Organisation mit der bereitgestellten Testdomain zu nutzen. Die Testdomain verwendet dieses Format: *example* .awsapps.com. Sie können die Test-Mail-Domain mit Amazon WorkMail und anderen unterstützten AWS Diensten verwenden, solange Sie aktivierte Benutzer in Ihrer WorkMail Amazon-Organisation haben. Sie können die Testdomain jedoch nicht für andere Zwecke verwenden. Die Testdomain kann möglicherweise von anderen Kunden registriert und verwendet werden, wenn Ihre WorkMail Amazon-Organisation nicht mindestens einen aktivierten Benutzer verwaltet.
- Amazon unterstützt WorkMail keine Verzeichnisse mit mehreren Regionen.

Themen

- Erstellen einer Organisation
- Die Details einer Organisation anzeigen
- Ein WorkSpaces Verzeichnis integrieren
- Organisationszustände und Beschreibungen

Erstellen einer Organisation

Erstellen Sie eine neue Organisation in der WorkMail Amazon-Konsole.

So erstellen Sie eine -Organisation:

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie in der Navigationsleiste Organisation aus.

   Die Seite Organizations wird angezeigt und zeigt Ihre Organisationen an, falls vorhanden.
3. Wählen Sie Organisation erstellen.
4. Wählen Sie unter E-Mail-Domäne die Domain aus, die für die E-Mail-Adressen in Ihrer Organisation verwendet werden soll:

   - Bestehende Route 53-Domain — Wählen Sie eine bestehende Domain aus, die Sie mit einer von Amazon Route 53 (Route 53) gehosteten Zone verwalten.
   - Neue Route 53-Domain — Registrieren Sie einen neuen Route 53-Domainnamen zur Verwendung bei Amazon WorkMail.
   - Externe Domain — Geben Sie eine bestehende Domain ein, die Sie mit einem externen DNS-Anbieter (Domain Name System) verwalten.
   - Kostenlose Testdomain — Verwenden Sie eine kostenlose Testdomain von Amazon WorkMail. Sie können Amazon WorkMail mithilfe einer Testdomain erkunden und dann später eine Domain zu Ihrer Organisation hinzufügen.
5. (Optional) Wenn Ihre Domain über Amazon Route 53 verwaltet wird, wählen Sie für Route 53 Hosted Zone Ihre Route 53-Domain aus.
6. Geben Sie unter Alias einen eindeutigen Alias für Ihre Organisation ein.
7. Wählen Sie Erweiterte Einstellungen und wählen Sie für Benutzerverzeichnis eine der folgenden Optionen aus:

   - Neues WorkMail Amazon-Verzeichnis erstellen — Erstellt ein neues Verzeichnis zum Hinzufügen und Verwalten Ihrer Benutzer.

- Bestehendes Verzeichnis verwenden — Verwendet ein vorhandenes Verzeichnis, um Ihre Benutzer zu verwalten, z. B. ein lokales Microsoft Active Directory, AWS Managed Active Directory oder Simple AD.

8. Wählen Sie für Verschlüsselung eine der folgenden Optionen aus:

   - Einen von Amazon WorkMail verwalteten Schlüssel verwenden — Erstellt einen neuen Verschlüsselungsschlüssel in Ihrem Konto.
   - Bestehenden KMS-Schlüssel verwenden — Verwendet einen vorhandenen KMS-Schlüssel, den Sie bereits erstellt haben AWS KMS.

9. Wählen Sie Organisation erstellen aus.

Wenn Sie eine externe Domain verwenden, überprüfen Sie diese, indem Sie Ihrem DNS-Dienst die entsprechenden Text- (TXT) - und Mail Exchanger- (MX) -Einträge hinzufügen. Mit TXT-Einträgen können Sie Notizen zum DNS-Dienst eingeben. MX-Einträge geben den Posteingangsserver an.

Stellen Sie sicher, dass Sie Ihre Domain als Standard für Ihre Organisation festlegen. Weitere Informationen erhalten Sie unter Verifizieren von Domänen und Auswählen der Standarddomäne.

Wenn Ihre Organisation aktiv ist, können Sie ihr Benutzer hinzufügen und deren E-Mail-Clients einrichten. Weitere Informationen finden Sie unter Hinzufügen eines Benutzers und E-Mail-Clients für Amazon einrichten WorkMail.

Die Details einer Organisation anzeigen

Jede Ihrer WorkMail Amazon-Organisationen kann eine Seite mit den Organisationsdetails anzeigen. Auf der Seite finden Sie Informationen über ihre Organisation, einschließlich Informationen, IDs die Sie zusammen mit der verwenden können AWS Command Line Interface. In den Nachrichten auf der Seite können Ihnen auch alle Schritte angezeigt werden, die zum Abschluss der Einrichtung und Organisation erforderlich sind, z. B. eine nicht verifizierte Domain oder das Fehlen von Benutzern. Die Nachrichten enthalten auch den ersten Schritt, den Sie ausführen, um einen bestimmten E-Mail-Client einzurichten.

Um die Details der Organisation einzusehen

1. Wählen Sie in der Navigationsleiste Organisation aus.

   Die Seite Organizations wird mit Ihren Organisationen angezeigt.

2. Wählen Sie die Organisation aus, die Sie anzeigen möchten.

Ein WorkSpaces Verzeichnis integrieren

Um Amazon WorkMail mit zu verwenden WorkSpaces, erstellen Sie mithilfe der folgenden Schritte ein kompatibles Verzeichnis.

Um ein kompatibles WorkSpaces Verzeichnis hinzuzufügen

1. Erstellen Sie ein kompatibles Verzeichnis mit WorkSpaces. WorkSpaces Anweisungen finden Sie unter Erste Schritte mit Amazon WorkSpaces Quick Setup im WorkSpaces Amazon-Administratorhandbuch.
2. Erstellen Sie in der WorkMail Amazon-Konsole Ihre WorkMail Amazon-Organisation und wählen Sie, ob Sie dafür Ihr vorhandenes Verzeichnis verwenden möchten. Weitere Informationen finden Sie unter Erstellen einer Organisation.

Organisationszustände und Beschreibungen

Nachdem Sie eine Organisation angelegt haben, kann sie einen der folgenden Zustände haben.

Status	Beschreibung
Aktiv	Ihre Organisation ist funktionsfähig und einsatzbereit.
Erstellen	Ein Workflow wird ausgeführt, um Ihre Organisation zu erstellen.
Fehlgeschlagen	Ihre Organisation konnte nicht erstellt werden.
Beeinträchtigt	Ihre Organisation ist gestört oder ein Problem wurde entdeckt.
Inaktiv	Ihre Organisation ist inaktiv.
Angefragt	Ihre Anforderung zur Erstellung einer Organisation steht in der Warteschlange und wartet darauf, erstellt zu werden.
Validierung	Alle Einstellungen für die Organisation werden einer Statusprüfung unterzogen.

Löschen einer Organisation

Wenn Sie Amazon nicht mehr WorkMail für die E-Mail Ihrer Organisation verwenden möchten, können Sie Ihre Organisation von Amazon löschen WorkMail.

> **Note**
>
> Dieser Vorgang kann nicht rückgängig gemacht werden. Sie können Ihre Postfachdaten nicht wiederherstellen, nachdem eine Organisation gelöscht wurde.

So löschen Sie eine Organisation

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie auf dem Bildschirm Organizations in der Liste der Organisationen die Organisation aus, die Sie löschen möchten, und wählen Sie Löschen.
3. Wählen Sie unter Organisation löschen aus, ob das bestehende Benutzerverzeichnis gelöscht oder beibehalten werden soll, und geben Sie dann den Namen der Organisation ein.
4. Wählen Sie Organisation löschen aus.

> **Note**
>
> Wenn Sie kein eigenes Verzeichnis für Amazon bereitgestellt haben WorkMail, erstellen wir eines für Sie. Wenn Sie dieses bestehende Verzeichnis beibehalten, wenn Sie die Organisation löschen, wird es Ihnen in Rechnung gestellt, sofern es nicht von Amazon verwendet wird WorkMail WorkDocs, oder WorkSpaces. Informationen zu den Kosten finden Sie auf der Seite über Preise für andere Verzeichnistypen.
> Um das Verzeichnis zu löschen, dürfen keine anderen AWS Anwendungen aktiviert werden. Weitere Informationen finden Sie unter Löschen eines Simple AD AD-Verzeichnisses oder Löschen eines AD Connector Connector-Verzeichnisses im AWS Directory Service Administratorhandbuch.

Möglicherweise erhalten Sie eine ungültige Amazon Simple Email Service (Amazon SES) -Regelsatz-Fehlermeldung, wenn Sie versuchen, eine Organisation zu löschen. Wenn Sie diesen Fehler erhalten, bearbeiten Sie die Amazon SES SES-Regel in der Amazon SES SES-Konsole und entfernen Sie den ungültigen Regelsatz. Die Regel, die Sie bearbeiten, sollte Ihre WorkMail Amazon-Organisations-ID im Regelnamen enthalten. Weitere Informationen zur Bearbeitung von Amazon SES SES-Regeln finden Sie unter Erstellen von Empfangsregeln im Amazon Simple Email Service Developer Guide.

Wenn Sie herausfinden müssen, welcher Regelsatz nicht gültig ist, speichern Sie zuerst die Regel. Für den Regelsatz wird eine Fehlermeldung angezeigt.

Eine E-Mail-Adresse finden

Sie können anhand von Benutzern, Ressourcen oder Gruppen herausfinden, ob eine E-Mail-Adresse in Ihrer Organisation verwendet wird.

Um eine E-Mail-Adresse zu finden

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen einer Organisation aus.
3. Wählen Sie auf der Seite Organisation die Option E-Mail-Adresse suchen aus.
4. Wählen Sie Search (Suchen) aus.

Mit Organisationseinstellungen arbeiten

In den folgenden Abschnitten wird erklärt, wie Sie die für WorkMail Amazon-Organisationen verfügbaren Einstellungen verwenden. Die von Ihnen ausgewählten Einstellungen gelten für die gesamte Organisation.

Themen

- Postfachmigration aktivieren
- Journaling aktivieren

- Interoperabilität aktivieren
- SMTP-Gateways aktivieren
- E-Mail-Fluss verwalten
- Durchsetzen von DMARC-Richtlinien für eingehende E-Mails

Postfachmigration aktivieren

Sie aktivieren die Postfachmigration, wenn Sie Postfächer von einer Quelle wie Microsoft Exchange oder G Suite Basic zu Amazon WorkMail übertragen möchten. Sie aktivieren die Migration als Teil eines größeren Migrationsprozesses. Weitere Informationen, einschließlich Anleitungen, finden Sie Zu Amazon migrieren WorkMail im Abschnitt Erste Schritte dieses Handbuchs.

Journaling aktivieren

Sie aktivieren das Journaling, um Ihre E-Mail-Kommunikation aufzuzeichnen. Wenn Sie Journaling verwenden, verwenden Sie in der Regel integrierte Archivierungs- und eDiscovery-Tools von Drittanbietern. Mithilfe von Journalen können Sie sicherstellen, dass Sie die Compliance-Vorschriften für Datenspeicherung, Datenschutz und Informationsschutz einhalten.

Weitere Informationen, einschließlich Anleitungen, finden Sie E-Mail-Journaling mit Amazon verwenden WorkMail im Abschnitt Erste Schritte dieses Handbuchs.

Interoperabilität aktivieren

Interoperabilität ermöglicht es Ihnen, von Microsoft Exchange zu migrieren und Amazon WorkMail als Teilmenge Ihrer Unternehmenspostfächer zu verwenden. Weitere Informationen, einschließlich Anleitungen, finden Sie Verfügbarkeitseinstellungen bei Amazon konfigurieren WorkMail im Abschnitt Erste Schritte dieses Handbuchs.

SMTP-Gateways aktivieren

Sie aktivieren SMTP-Gateways (Simple Mail Transfer Protocol) für die Verwendung mit Regeln für den Fluss ausgehender E-Mails. Mit den Regeln für den ausgehenden E-Mail-Fluss können Sie E-Mail-Nachrichten, die von Ihrer WorkMail Amazon-Organisation gesendet wurden, über ein SMTP-Gateway weiterleiten. Weitere Informationen finden Sie unter Regelaktionen für ausgehende E-Mails.

> **Note**
>
> SMTP-Gateways, die für Regeln für den Fluss ausgehender E-Mails konfiguriert sind, müssen Transport Layer Security (TLS) v1.2 unter Verwendung von Zertifikaten wichtiger Zertifizierungsstellen unterstützen. Nur grundlegende Authentifizierung wird unterstützt.

So konfigurieren Sie einen SMTP-Gateway

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen einer Organisation aus.
3. Klicken Sie im Navigationsbereich auf Organization settings (Organisationseinstellungen).

   Die Seite mit den Organisationseinstellungen wird mit einer Reihe von Registerkarten angezeigt.
4. Wählen Sie die Registerkarte SMTP-Gateways und anschließend Gateway erstellen.
5. Geben Sie Folgendes ein:

   - Gateway-Name — Geben Sie einen eindeutigen Namen ein.
   - Gateway-Adresse — Geben Sie den Hostnamen oder die IP-Adresse des Gateways ein.
   - Portnummer — Geben Sie die Portnummer des Gateways ein.
   - Benutzername — Geben Sie einen Benutzernamen ein.
   - Passwort — Geben Sie ein sicheres Passwort ein.
6. Wählen Sie Erstellen aus.

   Das SMTP-Gateway ist für die Verwendung mit E-Mail-Flussregeln für ausgehenden E-Mail-Verkehr verfügbar.

Wenn Sie ein SMTP-Gateway für die Verwendung mit einer Regel für den Fluss ausgehender E-Mails konfigurieren, versuchen ausgehende Nachrichten, die Regel mit einem SMTP-Gateway abzugleichen. Die Nachrichten, die der Regel entsprechen, werden an das entsprechende SMTP-Gateway weitergeleitet, das dann den Rest der E-Mail-Zustellung abwickelt.

Wenn Amazon WorkMail das SMTP-Gateway nicht erreichen kann, leitet das System die E-Mail-Nachricht an den Absender zurück. Wenn dies der Fall ist, folgen Sie den vorherigen Schritten, um die Gateway-Einstellungen zu korrigieren.

E-Mail-Fluss verwalten

Um die Verwaltung von E-Mails zu erleichtern, können Sie E-Mail-Flussregeln einrichten. E-Mail-Flussregeln können auf der Grundlage ihrer Adressen oder Domänen eine oder mehrere Aktionen für E-Mail-Nachrichten ausführen. Sie können E-Mail-Flussregeln für die E-Mail-Adressen oder Domänen von Absendern und Empfängern verwenden.

Wenn Sie eine E-Mail-Flussregel erstellen, geben Sie eine Regelaktion an, die auf eine E-Mail angewendet wird, wenn ein bestimmtes Regelmuster zutrifft.

Themen

- Regelaktionen für eingehende E-Mails
- Regelaktionen für ausgehende E-Mails
- Absender- und Empfängermuster
- Regeln für den E-Mail-Fluss erstellen
- E-Mail-Flussregeln bearbeiten
- Konfiguration AWS Lambda für Amazon WorkMail
- Zugriff auf die Amazon WorkMail Message Flow API verwalten
- Testen der E-Mail-Flussregel
- Entfernen der E-Mail-Flussregel

Regelaktionen für eingehende E-Mails

Mit E-Mail-Flussregeln lässt sich verhindern, dass ungewünschte E-Mails die Postfächer Ihrer Benutzer erreichen. Regeln für den Fluss eingehender E-Mails, auch Regelaktionen genannt, gelten automatisch für alle E-Mail-Nachrichten, die an Personen innerhalb Ihrer WorkMail Amazon-Organisation gesendet werden. Dies unterscheidet sich von den E-Mail-Regeln für einzelne Postfächer.

> **Note**
>
> Optional können Sie Regeln mit einer AWS Lambda Funktion verwenden, um eingehende E-Mails zu verarbeiten, bevor sie an die Postfächer Ihrer Benutzer zugestellt werden.

Weitere Informationen zur Verwendung von Lambda mit Amazon finden Sie WorkMail unterKonfiguration AWS Lambda für Amazon WorkMail. Weitere Informationen zu Lambda finden Sie im AWS Lambda Entwicklerhandbuch.

Regeln für den Fluss eingehender E-Mails, auch Regelaktionen genannt, gelten automatisch für alle E-Mail-Nachrichten, die an Personen innerhalb der WorkMail Amazon-Organisation gesendet werden. Dies unterscheidet sich von den E-Mail-Regeln für einzelne Postfächer.

Die folgenden Regelaktionen definieren, wie eingehende E-Mails gehandhabt werden. Für jede Regel geben Sie Absender- und Empfängermuster zusammen mit einer der folgenden Aktionen an.

Aktion	Beschreibung
E-Mail entfernen	Die E-Mail-Nachricht wird ignoriert. Sie wird nicht zugestellt und der Absender wird nicht über die Nichtzustellung informiert.
Senden einer Unzustellbarkeitsantwort	Die E-Mail-Nachricht wird nicht zugestellt, und der Absender wird in einer Bounce-Nachricht über die Nichtzustellung informiert.
Deliver to junk folder	Die E-Mail-Nachricht wird in den Spam- oder Junk-Ordnern der Benutzer zugestellt, auch wenn sie ursprünglich nicht vom Amazon-Sp am-Erkennungssystem als WorkMail Spam identifiziert wurde.
Standard	Die E-Mail-Nachricht wird zugestellt, nachdem sie vom WorkMail Amazon-Spam-Erkenn ungssystem geprüft wurde. Spam-E-Mail wird an den Junk-Ordner übermittelt. Alle anderen E-Mail-Nachrichten werden an den Posteinga ng zugestellt. Andere E-Mail-Flussregeln mit weniger spezifischen Absendermustern werden ignoriert . Um Ausnahmen zu domänenbasierten Regeln

Aktion	Beschreibung
	für den E-Mail-Verkehr hinzuzufügen, konfiguri eren Sie die Standardaktion mit einem spezifisc heren Absendermuster. Weitere Informationen finden Sie unter Absender- und Empfänger muster.
Never deliver to junk folder	Die E-Mail-Nachricht wird immer an die Posteingänge der Benutzer zugestellt, auch wenn sie vom Amazon-Spam-Erkennungssyste m als WorkMail Spam identifiziert wurde. **Important** Da Sie kein Spam-Erkennungssystem verwenden, könnten Sie Ihre Benutzer riskanten Inhalten von den von Ihnen angegebenen Adressen aussetzen.
Ausführen AWS Lambda	Leitet die E-Mail-Nachricht zur Verarbeitung an eine Lambda-Funktion weiter, bevor oder während sie an die Posteingänge der Benutzer zugestellt wird.

Note

Eingehende E-Mails werden zuerst an Amazon SES und dann an Amazon WorkMail zugestellt. Wenn Amazon SES eine eingehende E-Mail-Nachricht blockiert, gelten die Regelaktionen nicht. Amazon SES blockiert beispielsweise eine E-Mail-Nachricht, wenn ein bekannter Virus entdeckt wird oder wenn explizite IP-Filterregeln vorliegen. Die Angabe einer Regelaktion, wie z. B. Default (Standard), Deliver to junk folder (In Junk-Ordner verschieben) oder Never deliver to junk folder (Nie in Junk-Ordner verschieben) hat in diesem Fall keine Auswirkungen.

Regelaktionen für ausgehende E-Mails

Sie verwenden Regeln für den Fluss ausgehender E-Mails, um E-Mail-Nachrichten über SMTP-Gateways weiterzuleiten oder um Absender daran zu hindern, E-Mail-Nachrichten an bestimmte Empfänger zu senden. Weitere Informationen zu SMTP-Gateways finden Sie unter. SMTP-Gateways aktivieren

Sie können auch Regeln für den Fluss ausgehender E-Mails verwenden, um die E-Mail-Nachricht nach dem Senden an eine AWS Lambda Funktion zur Verarbeitung weiterzuleiten. Weitere Informationen zu Lambda finden Sie im AWS Lambda Entwicklerhandbuch.

Die folgenden Regelaktionen definieren, wie ausgehende E-Mails gehandhabt werden. Für jede Regel geben Sie Absender- und Empfängermuster zusammen mit einer der folgenden Aktionen an.

Aktion	Beschreibung
Standard	Die E-Mail-Nachricht wird über den normalen Nachrichtenfluss gesendet.
E-Mail entfernen	Die E-Mail-Nachricht wird gelöscht. Sie wird nicht gesendet und der Absender wird nicht benachrichtigt.
Senden einer Unzustellbarkeitsantwort	Die E-Mail-Nachricht wird nicht gesendet, und der Absender wird mit einer Nachricht darüber informiert, dass der Administrator die E-Mail-Nachricht blockiert hat.
Route to SMTP gateway (An SMTP-Gateway weiterleiten)	Die E-Mail-Nachricht wird über ein konfiguriertes SMTP-Gateway gesendet.
Führen Sie Lambda aus	Übergibt die E-Mail-Nachricht zur Verarbeitung an eine Lambda-Funktion, bevor oder während die E-Mail-Nachricht gesendet wird.

Absender- und Empfängermuster

Eine E-Mail-Flussregel kann für eine bestimmte E-Mail-Adresse oder für alle E-Mail-Adressen in einer bestimmten Domäne oder einem bestimmten Satz von Domänen gelten. Sie legen durch Definieren eines Musters fest, für welche E-Mail-Adressen eine Regel gilt.

Sowohl Absender- als auch Empfängermuster können eine der folgenden Formen haben:

- Eine E-Mail-Adresse entspricht einer einzelnen E-Mail-Adresse; zum Beispiel:

  ```
  mailbox@example.com
  ```

- Ein Domainname entspricht allen E-Mail-Adressen unter dieser Domain; zum Beispiel:

  ```
  example.com
  ```

- Eine Wildcard-Domain entspricht allen E-Mail-Adressen unter dieser Domain und all ihren Subdomänen. Ein Platzhalter erscheint nur am Anfang einer Domäne, zum Beispiel:

  ```
  *.example.com
  ```

- Ein Stern entspricht allen E-Mail-Adressen unter einer beliebigen Domain.

  ```
  *
  ```

> **Note**
>
> Das Symbol + ist innerhalb von Absender- oder Empfängermustern nicht gültig.

Für eine Regel können mehrere Muster angegeben werden. Weitere Informationen erhalten Sie unter Regelaktionen für eingehende E-Mails und Regelaktionen für ausgehende E-Mails.

Regeln für den Fluss eingehender E-Mails werden angewendet, wenn entweder der `From` Header `Sender` oder in einer eingehenden E-Mail-Nachricht beliebigen Mustern entspricht. Falls vorhanden, wird die `Sender`-Adresse zuerst abgeglichen. Die `From`-Adresse wird abgeglichen, wenn es keinen `Sender`-Header gibt oder wenn der `Sender`-Header keiner Regel entspricht. Wenn es mehrere Empfänger für die E-Mail-Nachricht gibt, die unterschiedlichen Regeln entsprechen, gilt jede Regel für die entsprechenden Empfänger.

Regeln für den Fluss ausgehender E-Mails werden angewendet, wenn der Empfänger und entweder der `From` Header `Sender` oder in der Kopfzeile einer ausgehenden E-Mail-Nachricht beliebigen Mustern entsprechen. Wenn es mehrere Empfänger für die E-Mail-Nachricht gibt, die unterschiedlichen Regeln entsprechen, gilt jede Regel für die entsprechenden Empfänger.

Wenn mehrere Regeln zutreffen, wird die Aktion der spezifischsten Regel angewendet. So hat beispielsweise eine Regel für eine bestimmte E-Mail-Adresse Priorität gegenüber einer Regel für eine gesamte Domain. Wenn mehrere Regeln dasselbe Maß an Spezifität aufweisen, wird die Aktion, die die größte Einschränkung darstellt, ausgeführt. Beispiel: Eine Drop-Aktion hat Vorrang vor einer Bounce-Aktion. Die Rangfolge für Aktionen entspricht der Reihenfolge, in der sie in Regelaktionen für eingehende E-Mails undRegelaktionen für ausgehende E-Mails aufgeführt werden.

> **Note**
>
> Seien Sie vorsichtig, wenn Sie Regeln mit überlappenden Absendermustern mit Drop- oder Bounce-Aktionen erstellen. Eine unerwartete Rangfolge könnte dazu führen, dass viele eingehende E-Mail-Nachrichten nicht zugestellt werden.

Regeln für den E-Mail-Fluss erstellen

E-Mail-Flussregeln wenden Regelaktionen auf eingehende und ausgehende E-Mail-Nachrichten an. Die Aktionen werden angewendet, wenn Nachrichten einem bestimmten Muster entsprechen. Neue Regeln für den E-Mail-Fluss werden sofort wirksam.

Um Regeln für den E-Mail-Fluss zu erstellen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen einer Organisation aus.
3. Klicken Sie im Navigationsbereich auf Organization settings (Organisationseinstellungen).

   Die Seite mit den Organisationseinstellungen wird mit einer Reihe von Registerkarten angezeigt. Auf dieser Seite können Sie Regeln für eingehenden oder ausgehenden Datenverkehr erstellen. In den folgenden Schritten wird erklärt, wie Sie beide Typen erstellen.

Um Regeln für eingehenden Datenverkehr zu erstellen

1. Wählen Sie die Registerkarte Regeln für eingehende Nachrichten und dann Erstellen aus.
2. Geben Sie im Feld Regelname einen eindeutigen Namen ein.
3. Öffnen Sie unter Aktion die Liste und wählen Sie eine Aktion aus. Jedes Element in der Liste enthält eine Beschreibung und einige enthalten Links zu weiteren Informationen.

> **Note**
>
> Wenn Sie die Aktion „Lambda ausführen“ wählen, werden zusätzliche Steuerelemente angezeigt: Informationen zur Verwendung dieser Steuerelemente finden Sie im nächsten Abschnitt. Konfiguration AWS Lambda für Amazon WorkMail

4. Geben Sie unter Absenderdomänen oder Adressen die Absenderdomänen oder Adressen ein, für die die Regel gelten soll.
5. Geben Sie unter Zieldomänen oder -adressen eine beliebige Kombination aus Zieldomänen und E-Mail-Adressen ein.
6. Wählen Sie Erstellen aus.

Um Regeln für ausgehenden Datenverkehr zu erstellen

1. Wählen Sie die Registerkarte Ausgehende Regeln und dann Erstellen aus.
2. Geben Sie im Feld Regelname einen eindeutigen Namen ein.
3. Öffnen Sie unter Aktion die Liste und wählen Sie eine Aktion aus. Jedes Element in der Liste enthält eine Beschreibung und einige enthalten Links zu weiteren Informationen.

> **Note**
>
> Wenn Sie die Aktion „Lambda ausführen“ wählen, werden zusätzliche Steuerelemente angezeigt. Informationen zur Verwendung dieser Steuerelemente finden Sie im nächsten Abschnitt. Konfiguration AWS Lambda für Amazon WorkMail

4. Geben Sie unter Absenderdomänen oder Adressen eine beliebige Kombination aus gültigen Absenderdomänen und E-Mail-Adressen ein.
5. Geben Sie unter Zieldomänen oder -adressen eine beliebige Kombination aus gültigen Zieldomänen und E-Mail-Adressen ein.

6. Wählen Sie Erstellen aus.

   Sie können die neu erstellte E-Mail-Flussregeln testen. Weitere Informationen finden Sie unter Testen der E-Mail-Flussregel.

E-Mail-Flussregeln bearbeiten

Sie bearbeiten E-Mail-Flussregeln immer dann, wenn Sie eine oder mehrere Regelaktionen für E-Mail-Nachrichten ändern müssen. Die Schritte in diesem Abschnitt gelten für eingehende und ausgehende E-Mail-Nachrichten.

Um Regeln für den E-Mail-Fluss zu bearbeiten

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen einer Organisation aus.
3. Klicken Sie im Navigationsbereich auf Organization settings (Organisationseinstellungen).

   Die Seite mit den Organisationseinstellungen wird mit einer Reihe von Registerkarten angezeigt.
4. Wählen Sie die Registerkarten Eingehende Regeln oder Ausgehende Regeln.
5. Wählen Sie das Optionsfeld neben der Regel, die Sie ändern möchten, und wählen Sie dann Bearbeiten aus.
6. Ändern Sie die Aktion oder Aktionen in der Regel nach Bedarf und wählen Sie dann Speichern aus.

Konfiguration AWS Lambda für Amazon WorkMail

Verwenden Sie die Aktion Lambda ausführen in den Regeln für den Fluss eingehender und ausgehender E-Mails, um E-Mail-Nachrichten, die den Regeln entsprechen, zur Verarbeitung an eine AWS Lambda Funktion weiterzuleiten.

Wählen Sie aus den folgenden Konfigurationen für eine Aktion „Lambda ausführen“ in Amazon WorkMail.

Lambda-Konfiguration für synchrone Ausführung

E-Mail-Nachrichten, die der Flussregel entsprechen, werden zur Verarbeitung an eine Lambda-Funktion übergeben, bevor sie gesendet oder zugestellt werden. Verwenden Sie diese Konfiguration, um E-Mail-Inhalte zu ändern. Sie können auch den eingehenden oder ausgehenden E-Mail-Fluss für verschiedene Anwendungsfälle steuern. Beispielsweise kann eine an eine Lambda-Funktion übergebene Regel die Zustellung vertraulicher E-Mail-Nachrichten blockieren, Anlagen entfernen oder Haftungsausschlüsse hinzufügen.

Lambda-Konfiguration für asynchrone Ausführung

E-Mail-Nachrichten, die der Flow-Regel entsprechen, werden an eine Lambda-Funktion zur Verarbeitung übergeben, während sie gesendet oder zugestellt werden. Diese Konfiguration hat keine Auswirkungen auf die E-Mail-Zustellung und wird für Aufgaben wie das Sammeln von Metriken für eingehende oder ausgehende E-Mail-Nachrichten verwendet.

Unabhängig davon, ob Sie sich für eine synchrone oder asynchrone Konfiguration entscheiden, enthält das an Ihre Lambda-Funktion übergebene Ereignisobjekt Metadaten für das eingehende oder ausgehende E-Mail-Ereignis. Sie können auch die Nachrichten-ID in den Metadaten verwenden, um auf den vollständigen Inhalt der E-Mail-Nachricht zuzugreifen. Weitere Informationen finden Sie unter Nachrichteninhalt wird abgerufen mit AWS Lambda. Weitere Informationen zu E-Mail-Ereignissen finden Sie unter Lambda-Ereignisdaten.

Weitere Informationen über E-Mail-Flussregeln für ein- und ausgehenden E-Mail-Verkehr finden Sie unter E-Mail-Fluss verwalten. Weitere Informationen zu Lambda finden Sie im AWS Lambda Entwicklerhandbuch.

> **Note**
>
> Derzeit verweisen Lambda-E-Mail-Flussregeln nur auf Lambda-Funktionen in derselben AWS-Region und AWS-Konto wie die WorkMail Amazon-Organisation, die konfiguriert wird.

Erste Schritte mit AWS Lambda für Amazon WorkMail

Um mit der Nutzung AWS Lambda mit Amazon zu beginnen WorkMail, empfehlen wir, die WorkMail Hello World Lambda-Funktion von AWS Serverless Application Repository auf Ihrem Konto bereitzustellen. Die Funktion verfügt über alle erforderlichen Ressourcen und die für

Sie konfigurierten Berechtigungen. Weitere Beispiele finden Sie im amazon-workmail-lambda-templatesRepository unter GitHub.

Wenn Sie Ihre eigene Lambda-Funktion erstellen möchten, müssen Sie Berechtigungen mit der AWS Command Line Interface (AWS CLI) konfigurieren. Gehen Sie im folgenden Beispielbefehl wie folgt vor:

- `MY_FUNCTION_NAME`Ersetzen Sie durch den Namen Ihrer Lambda-Funktion.
- `REGION`Ersetzen Sie es durch Ihre Amazon WorkMail AWS-Region. Zu den verfügbaren WorkMail Amazon-Regionen gehören `us-east-1` (USA Ost (Nord-Virginia)), `us-west-2` (USA West (Oregon)) und `eu-west-1` (Europa (Irland)).
- Ersetzen Sie es `AWS_ACCOUNT_ID` durch Ihre 12-stellige AWS-Konto ID.
- `WORKMAIL_ORGANIZATION_ID`Ersetzen Sie es durch Ihre WorkMail Amazon-Organisations-ID. Sie finden es auf der Karte für Ihre Organisation auf der Seite Organizations.

```
aws --region REGION lambda add-permission --function-name MY_FUNCTION_NAME
--statement-id AllowWorkMail
--action "lambda:InvokeFunction"
--principal workmail.REGION.amazonaws.com
--source-arn
 arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID
```

Weitere Informationen zur Verwendung von AWS CLI finden Sie im AWS Command Line Interface Benutzerhandbuch.

Konfiguration synchroner Run-Lambda-Regeln

Um eine synchrone Lambda-Regel auszuführen zu konfigurieren, erstellen Sie eine E-Mail-Flussregel mit der Aktion Lambda ausführen und aktivieren Sie das Kontrollkästchen Synchron ausführen. Weitere Informationen zum Erstellen von Nachrichtenflussregeln finden Sie unter Regeln für den E-Mail-Fluss erstellen.

Um die Erstellung der synchronen Regel abzuschließen, fügen Sie den Lambda Amazon Resource Name (ARN) hinzu und konfigurieren Sie die folgenden Optionen.

Fallback-Aktion

Die Aktion, die Amazon WorkMail anwendet, wenn die Lambda-Funktion nicht ausgeführt werden kann. Diese Aktion gilt auch für allRecipients, die in der Lambda-Antwort nicht enthalten sind, wenn das AllRecipients-Flag nicht gesetzt ist. Die Fallback-Aktion kann keine weitere Lambda-Aktion sein.

Regel-Timeout (in Minuten)

Der Zeitraum, in dem die Lambda-Funktion erneut versucht wird, falls Amazon sie WorkMail nicht aufrufen kann. Die Fallback-Aktion wird am Ende dieses Zeitraums angewendet.

> **Note**
>
> Lambda-Regeln für synchronen Lauf unterstützen nur die ***** Zielbedingung.

Lambda-Ereignisdaten

Die Lambda-Funktion wird mithilfe der folgenden Ereignisdaten ausgelöst. Die Darstellung der Daten hängt davon ab, welche Programmiersprache für die Lambda-Funktion verwendet wird.

```
{
    "summaryVersion": "2018-10-10",
    "envelope": {
        "mailFrom" : {
            "address" : "from@example.com"
        },
        "recipients" : [
           { "address" : "recipient1@example.com" },
           { "address" : "recipient2@example.com" }
        ]
    },
    "sender" : {
        "address" :  "sender@example.com"
    },
    "subject" : "Hello From Amazon WorkMail!",
    "messageId": "00000000-0000-0000-0000-000000000000",
    "invocationId": "00000000000000000000000000000000",
    "flowDirection": "INBOUND",
    "truncated": false
```

```
}
```

Das Ereignis-JSON enthält die folgenden Daten.

summaryVersion

Die Versionsnummer für`LambdaEventData`. Dies wird nur aktualisiert, wenn Sie eine rückwärtsinkompatible Änderung in `LambdaEventData` vornehmen.

envelope

Der Umschlag der E-Mail-Nachricht, der Folgendes umfasst: Felder.

mailFrom

Die Adresse für Von. Dies ist in der Regel die E-Mail-Adresse des Benutzers, der die E-Mail-Nachricht gesendet hat. Wenn der Benutzer die E-Mail-Nachricht als ein anderer Benutzer oder im Auftrag eines anderen Benutzers gesendet hat, gibt das Feld mailFrom die E-Mail-Adresse des Benutzers zurück, in dessen Auftrag die E-Mail-Nachricht gesendet wurde, und nicht die E-Mail-Adresse des tatsächlichen Absenders.

recipients

Eine Liste der Empfänger-E-Mail-Adressen. Amazon unterscheidet WorkMail nicht zwischen To, CC oder BCC.

> **Note**
>
> Bei Regeln für den E-Mail-Verkehr für eingehende E-Mails enthält diese Liste Empfänger in allen Domains der WorkMail Amazon-Organisation, in der Sie die Regel erstellen. Die Lambda-Funktion wird für jede SMTP-Konversation des Absenders separat aufgerufen, und das Empfängerfeld listet die Empfänger dieser SMTP-Konversation auf. Empfänger mit externen Domänen werden nicht eingeschlossen.

sender

Die E-Mail-Adresse des Benutzers, der die E-Mail-Nachricht im Namen eines anderen Benutzers gesendet hat. Dieses Feld wird nur festgelegt, wenn eine E-Mail-Nachricht im Namen eines anderen Benutzers gesendet wird.

subject

Die E-Mail-Betreffzeile. Wird abgeschnitten, wenn die Beschränkung auf 256 Zeichen überschritten wird.

messageId

Eine eindeutige ID, die für den Zugriff auf den gesamten Inhalt der E-Mail-Nachricht verwendet wird, wenn das Amazon WorkMail Message Flow SDK verwendet wird.

invocationId

Die ID für einen eindeutigen Lambda-Aufruf. Diese ID bleibt gleich, wenn eine Lambda-Funktion mehrmals für dieselbe LambdaEventDataaufgerufen wird. Verwenden Sie diese Option, um Wiederholungen zu erkennen und Duplizierungen zu vermeiden.

flowDirection

Gibt die Richtung des E-Mail-Flusses an, entweder EINGEHEND oder AUSGEHEND.

truncated

Gilt für die Nutzlastgröße und nicht für die Länge der Betreffzeile. Bei dem Wert `true` überschreitet die Nutzlast das 128-KB-Limit, sodass die Liste von Empfängern abgeschnitten wird, um dem Limit zu entsprechen.

Lambda-Antwortschema für synchrone Ausführung

Wenn eine E-Mail-Flussregel mit einer synchronen Aktion „Lambda ausführen“ mit einer eingehenden oder ausgehenden E-Mail-Nachricht übereinstimmt, WorkMail ruft Amazon die konfigurierte Lambda-Funktion auf und wartet auf die Antwort, bevor Maßnahmen für die E-Mail-Nachricht ergriffen werden. Die Lambda-Funktion gibt eine Antwort gemäß einem vordefinierten Schema zurück, das die Aktionen, Aktionstypen, anwendbaren Parameter und Empfänger auflistet, für die die Aktion gilt.

Das folgende Beispiel zeigt eine synchrone Run Lambda-Antwort. Die Antworten variieren je nach der für die Lambda-Funktion verwendeten Programmiersprache.

```
{
    "actions": [
      {
        "action" : {
          "type": "string",
```

```
          "parameters": { various }
        },
        "recipients": [list of strings],
        "allRecipients": boolean
      }
    ]
}
```

Das Antwort-JSON enthält die folgenden Daten.

action

Die Aktion, die für die Empfänger ausgeführt werden soll.

Typ

Der Aktionstyp. Aktionstypen werden für asynchrone Run Lambda-Aktionen nicht zurückgegeben.

Zu den Aktionstypen für eingehende Regeln gehören BOUNCE, DROP, DEFAULT, BYPASS_SPAM_CHECK und MOVE_TO_JUNK. Weitere Informationen finden Sie unter Regelaktionen für eingehende E-Mails.

Zu den Aktionstypen für ausgehende Regeln gehören BOUNCE, DROP und DEFAULT. Weitere Informationen finden Sie unter Regelaktionen für ausgehende E-Mails.

Parameter

Zusätzliche Aktionsparameter. Unterstützt für den BOUNCE-Aktionstyp als JSON-Objekt mit dem Schlüssel bounceMessage und dem Wert string. Diese Unzustellbarkeitsnachricht wird verwendet, um die Unzustellbarkeits-E-Mail-Nachricht zu erstellen.

recipients

Liste der E-Mail-Adressen, für die die Aktion durchgeführt werden soll. Sie können der Antwort neue Empfänger hinzufügen, auch wenn sie nicht in der ursprünglichen Empfängerliste enthalten waren. Dieses Feld ist nicht erforderlich, wenn allRecipients für eine Aktion „true“ ist.

> **Note**
>
> Wenn eine Lambda-Aktion für eingehende E-Mails aufgerufen wird, können Sie nur neue Empfänger hinzufügen, die aus Ihrer Organisation stammen. Die neuen Empfänger werden der Antwort als BCC hinzugefügt.

allRecipients

Wenn wahr, wird die Aktion auf alle Empfänger angewendet, die keiner anderen spezifischen Aktion in der Lambda-Antwort unterliegen.

Limits für Lambda-Aktionen bei synchroner Ausführung

Die folgenden Beschränkungen gelten, wenn Amazon Lambda-Funktionen für synchrone Run Lambda-Aktionen WorkMail aufruft:

- Lambda-Funktionen müssen innerhalb von 15 Sekunden antworten oder als fehlgeschlagene Aufrufe behandelt werden.

> **Note**
>
> Das System wiederholt den Aufruf für das von Ihnen angegebene Regel-Timeout-Intervall.

- Lambda-Funktionsantworten bis zu 256 KB sind zulässig.
- Bis zu 10 eindeutige Aktionen sind in der Antwort zulässig. Aktionen, die größer als 10 sind, unterliegen der konfigurierten Fallback-Aktion.
- Für ausgehende Lambda-Funktionen sind bis zu 500 Empfänger zulässig.
- Der maximale Wert für Regel-Timeout beträgt 240 Minuten. Wenn der Mindestwert 0 konfiguriert ist, gibt es keine erneuten Versuche, bevor Amazon die Fallback-Aktion WorkMail anwendet.

Fehler bei der Aktion „Synchronous Run Lambda“

Wenn Amazon Ihre Lambda-Funktion aufgrund eines Fehlers, einer ungültigen Antwort oder eines Lambda-Timeouts nicht aufrufen WorkMail kann, WorkMail wiederholt Amazon den Aufruf mit einem exponentiellen Backoff, der die Verarbeitungsrate verringert, bis der Regel-Timeout-Zeitraum abgelaufen ist. Anschließend wird die Fallback-Aktion auf alle Empfänger der E-Mail-Nachricht angewendet. Weitere Informationen finden Sie unter Konfiguration synchroner Run-Lambda-Regeln.

Beispiel für synchrone Run-Lambda-Antworten

Die folgenden Beispiele veranschaulichen die Struktur gängiger synchroner Run-Lambda-Antworten.

Example : Entfernen angegebene Empfänger aus einer E-Mail-Nachricht

Das folgende Beispiel zeigt die Struktur einer synchronen Run Lambda-Antwort zum Entfernen von Empfängern aus einer E-Mail-Nachricht.

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      },
      {
        "action": {
          "type": "DROP"
        },
        "recipients": [
          "drop-recipient@example.com"
        ]
      }
    ]
}
```

Example : Bounce mit einer benutzerdefinierten E-Mail-Nachricht

Das folgende Beispiel zeigt die Struktur einer synchronen Run Lambda-Antwort für das Bouncing mit einer benutzerdefinierten E-Mail-Nachricht.

```
{
    "actions" : [
      {
        "action" : {
          "type": 'BOUNCE',
          "parameters": {
            "bounceMessage" : "Email in breach of company policy."
          }
        },
        "allRecipients": true
      }
    ]
}
```

Example : Hinzufügen von Empfängern zu einer E-Mail-Nachricht

Das folgende Beispiel zeigt die Struktur einer synchronen Run Lambda-Antwort zum Hinzufügen von Empfängern zur E-Mail-Nachricht. Dadurch werden die Felder An oder CC der E-Mail-Nachricht nicht aktualisiert.

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
        },
        "recipients": [
          "new-recipient@example.com"
         ]
      },
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      }
    ]
}
```

Weitere Codebeispiele für die Erstellung von Lambda-Funktionen für Run Lambda-Aktionen finden Sie unter Amazon WorkMail Lambda-Vorlagen.

Weitere Informationen zur Verwendung von Lambda mit Amazon WorkMail

Sie können auch auf den vollständigen Inhalt der E-Mail-Nachricht zugreifen, die die Lambda-Funktion auslöst. Weitere Informationen finden Sie unter Nachrichteninhalt wird abgerufen mit AWS Lambda.

Nachrichteninhalt wird abgerufen mit AWS Lambda

Nachdem Sie eine AWS Lambda Funktion zur Verwaltung von E-Mail-Flüssen für Amazon konfiguriert haben WorkMail, können Sie auf den vollständigen Inhalt der E-Mail-Nachrichten zugreifen, die mit Lambda verarbeitet werden. Weitere Informationen zu den ersten Schritten mit Lambda für Amazon finden Sie WorkMail unterKonfiguration AWS Lambda für Amazon WorkMail.

Verwenden Sie die `GetRawMessageContent` Aktion in der Amazon WorkMail Message Flow API, um auf den vollständigen Inhalt von E-Mail-Nachrichten zuzugreifen. Die E-Mail-Nachrichten-ID, die beim Aufruf an Ihre Lambda-Funktion übergeben wird, sendet eine Anfrage an die API. Anschließend antwortet die API mit dem vollständigen MIME-Inhalt der E-Mail-Nachricht. Weitere Informationen finden Sie unter Amazon WorkMail Message Flow in der Amazon WorkMail API-Referenz.

Das folgende Beispiel zeigt, wie eine Lambda-Funktion, die die Python-Laufzeitumgebung verwendet, den vollständigen Nachrichteninhalt abrufen kann.

> **Tip**
>
> Wenn Sie zunächst die Amazon WorkMail Hello World Lambda-Funktion über Ihr Konto bereitstellen, erstellt das System in Ihrem Konto eine Lambda-Funktion mit allen erforderlichen Ressourcen und Berechtigungen. AWS Serverless Application Repository Anschließend können Sie je nach Anwendungsfall Ihre Geschäftslogik zur Lambda-Funktion hinzufügen.

```
import boto3
import email
import os

def email_handler(event, context):
    workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
    msg_id = event['messageId']
    raw_msg = workmail.get_raw_message_content(messageId=msg_id)

    parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())
    print(parsed_msg)
```

Ausführlichere Beispiele für Methoden zur Analyse des Inhalts von Nachrichten, die gerade übertragen werden, finden Sie im Repository unter. amazon-workmail-lambda-templates GitHub

> **Note**
>
> Sie verwenden die Amazon WorkMail Message Flow API nur, um auf E-Mail-Nachrichten zuzugreifen, die gerade übertragen werden. Sie können nur innerhalb von 24 Stunden nach dem Senden oder Empfangen auf die Nachrichten zugreifen. Verwenden Sie eines der anderen von Amazon unterstützten Protokolle, wie IMAP oder Exchange Web Services

(EWS) WorkMail, um programmgesteuert auf Nachrichten im Postfach eines Benutzers zuzugreifen.

Nachrichteninhalte mit AWS Lambda aktualisieren

Nachdem Sie eine synchrone AWS Lambda Funktion zur Verwaltung von E-Mail-Datenströmen konfiguriert haben, können Sie die `PutRawMessageContent` Aktion in der Amazon WorkMail Message Flow-API verwenden, um den Inhalt von E-Mail-Nachrichten während der Übertragung zu aktualisieren. Weitere Informationen zu den ersten Schritten mit Lambda-Funktionen für Amazon finden Sie WorkMail unterKonfiguration synchroner Run-Lambda-Regeln. Weitere Informationen zur API finden Sie unter PutRawMessageContent.

> **Note**
>
> Die PutRawMessageContent API benötigt boto3 1.17.8, oder Sie können Ihrer Lambda-Funktion eine Ebene hinzufügen. Informationen zum Herunterladen der richtigen Boto3-Version finden Sie auf der Boto-Seite unter. GitHub Weitere Informationen zum Hinzufügen von Ebenen finden Sie unter Eine Funktion für die Verwendung von Ebenen konfigurieren. Hier ist ein Beispiel für eine Ebene:`"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`. Ersetzen Sie in diesem Beispiel `${AWS::Region}` durch eine entsprechende AWS-Region, z. B. us-east-1.

> **Tip**
>
> Wenn Sie zunächst die Amazon WorkMail Hello World Lambda-Funktion aus dem AWS Serverless Application Repository für Ihr Konto bereitstellen, erstellt das System in Ihrem Konto eine Lambda-Funktion mit den erforderlichen Ressourcen und Berechtigungen. Anschließend können Sie der Lambda-Funktion Geschäftslogik hinzufügen, die auf Ihren Anwendungsfällen basiert.

Denken Sie dabei an Folgendes:

- Verwenden Sie die GetRawMessageContentAPI, um den ursprünglichen Nachrichteninhalt abzurufen. Weitere Informationen finden Sie unter Nachrichteninhalt wird abgerufen mit AWS Lambda.

- Sobald Sie die ursprüngliche Nachricht haben, ändern Sie den MIME-Inhalt. Wenn Sie fertig sind, laden Sie die Nachricht in einen Amazon Simple Storage Service (Amazon S3) -Bucket in Ihrem Konto hoch. Stellen Sie sicher, dass der S3-Bucket dasselbe verwendet AWS-Konto wie Ihr WorkMail Amazon-Betrieb und dass er dieselbe AWS-Region wie Ihre API-Aufrufe verwendet.
- Damit Amazon WorkMail Anfragen bearbeiten kann, muss Ihr S3-Bucket über die richtige Richtlinie verfügen, um auf das S3-Objekt zugreifen zu können. Weitere Informationen finden Sie unter Example S3 policy.
- Verwenden Sie die PutRawMessageContentAPI, um den aktualisierten Nachrichteninhalt zurück an Amazon zu senden WorkMail.

> **Note**
>
> Die `PutRawMessageContent` API stellt sicher, dass der MIME-Inhalt der aktualisierten Nachricht den RFC-Standards sowie den im RawMessageContentDatentyp genannten Kriterien entspricht. E-Mails, die an Ihre WorkMail Amazon-Organisation eingehen, erfüllen diese Standards nicht immer, sodass die `PutRawMessageContent` API sie möglicherweise ablehnt. In solchen Fällen finden Sie in der zurückgegebenen Fehlermeldung weitere Informationen zur Behebung von Problemen.

Example Beispiel für eine S3-Richtlinie

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Service": "workmail.REGION.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::My-Test-S3-Bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "AWS_ACCOUNT_ID"
                },
                "Bool": {
```

```
                    "aws:SecureTransport": "true"
                },
                "ArnLike": {
                    "aws:SourceArn":
 "arn:aws:workmailmessageflow:REGION:AWS_ACCOUNT_ID:message/WORKMAIL_ORGANIZATION_ID/*"
                }
            }
        }
    ]
}
```

Das folgende Beispiel zeigt, wie eine Lambda-Funktion die Python-Laufzeit verwendet, um den Betreff einer E-Mail-Nachricht während der Übertragung zu aktualisieren.

```
    import boto3
    import os
    import uuid
    import email

    def email_handler(event, context):
        workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
        s3 = boto3.client('s3', region_name=os.environ["AWS_REGION"])

        msg_id = event['messageId']
        raw_msg = workmail.get_raw_message_content(messageId=msg_id)
        parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())

        # Updating subject. For more examples, see https://github.com/aws-samples/
amazon-workmail-lambda-templates.
        parsed_msg.replace_header('Subject', "New Subject Updated From Lambda")

        # Store updated email in S3
        key = str(uuid.uuid4());
        s3.put_object(Body=parsed_msg.as_bytes(), Bucket="amzn-s3-demo-bucket",
 Key=key)

        # Update the email in WorkMail
        s3_reference = {
            'bucket': "amzn-s3-demo-bucket",
            'key': key
        }
```

```
        content = {
            's3Reference': s3_reference
        }
        workmail.put_raw_message_content(messageId=msg_id, content=content)
```

Weitere Beispiele für Methoden zur Analyse des Inhalts von Nachrichten während der Übertragung finden Sie im amazon-workmail-lambda-templatesRepository unter. GitHub

Zugriff auf die Amazon WorkMail Message Flow API verwalten

Verwenden Sie AWS Identity and Access Management (IAM) -Richtlinien, um den Zugriff auf die Amazon WorkMail Message Flow API zu verwalten.

Die Amazon WorkMail Message Flow API arbeitet mit einem einzigen Ressourcentyp, einer E-Mail-Nachricht während der Übertragung. Jeder E-Mail-Nachricht, die übertragen wird, ist ein eindeutiger Amazon-Ressourcenname (ARN) zugeordnet.

Das folgende Beispiel zeigt die Syntax eines ARN, der einer E-Mail-Nachricht während der Übertragung zugeordnet ist.

```
arn:aws:workmailmessageflow:region:account:message/organization/context/messageID
```

Zu den Feldern im vorherigen Beispiel, die geändert werden können, gehören die folgenden:

- Region — Die AWS-Region für Ihre WorkMail Amazon-Organisation.
- Konto — Die AWS-Konto ID für Ihre WorkMail Amazon-Organisation.
- Organisation — Ihre WorkMail Amazon-Organisations-ID.
- Kontext — Gibt an, ob die Nachricht `incoming` an Ihre Organisation gerichtet ist oder `outgoing` von ihr stammt.
- Nachrichten-ID — Die eindeutige E-Mail-Nachrichten-ID, die als Eingabe an Ihre Lambda-Funktion übergeben wird.

Das folgende Beispiel enthält ein Beispiel IDs für einen ARN, der einer eingehenden E-Mail-Nachricht während der Übertragung zugeordnet ist.

```
arn:aws:workmailmessageflow:us-east-1:111122223333:message/m-
n1pq2345678r901st2u3vx45x6789yza/incoming/d1234567-8e90-1f23-456g-hjk7lmnop8q9
```

Sie können diese ARNs als Ressourcen im `Resource` Abschnitt Ihrer IAM-Benutzerrichtlinien verwenden, um den Zugriff auf WorkMail Amazon-Nachrichten während der Übertragung zu verwalten.

Beispiel für IAM-Richtlinien für den Zugriff auf den WorkMail Amazon-Nachrichtenfluss

Die folgende Beispielrichtlinie gewährt einer IAM-Entität vollen Lesezugriff auf alle eingehenden und ausgehenden Nachrichten für jede WorkMail Amazon-Organisation in Ihrer. AWS-Konto

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

Wenn Sie mehrere Organisationen in Ihrem Unternehmen haben AWS-Konto, können Sie den Zugriff auch auf eine oder mehrere Organisationen beschränken. Dies ist nützlich, wenn bestimmte Lambda-Funktionen nur für bestimmte Organisationen verwendet werden sollen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/*",
            "Effect": "Allow"
        }
    ]
}
```

Sie können den Zugriff auf Nachrichten auch abhängig davon gewähren, ob sie `incoming` oder `outgoing` in Bezug auf Ihre Organisation sind. Hierzu verwenden Sie die Qualifizierer `incoming` oder `outgoing` im ARN.

Die folgende Beispielrichtlinie gewährt Zugriff nur auf Nachrichten, die bei Ihrer Organisation eingehen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/incoming/*",
            "Effect": "Allow"
        }
    ]
}
```

Die folgende Beispielrichtlinie gewährt einer IAM-Entität vollen Lese- und Aktualisierungszugriff auf alle eingehenden und ausgehenden Nachrichten für jede WorkMail Amazon-Organisation in Ihrer. AWS-Konten

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent",
                "workmailmessageflow:PutRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

Testen der E-Mail-Flussregel

Um Ihre aktuelle Regelkonfiguration zu überprüfen, können Sie testen, wie sich die Konfiguration gegenüber bestimmten E-Mail-Adressen verhält.

So testen Sie eine E-Mail-Flussregel

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Organization settings (Organisationseinstellungen) und Inbound/Outbound rules (Regeln für ein-/ausgehenden Datenverkehr) aus.
4. Geben Sie neben Test configuration (Testkonfiguration) die vollständige E-Mail-Adresse sowohl des Absenders als auch des Empfängers ein, die Sie testen möchten.
5. Wählen Sie Test aus. Die Aktion, die für die angegebene E-Mail-Adresse durchgeführt wird, wird angezeigt.

Entfernen der E-Mail-Flussregel

Wenn Sie eine E-Mail-Flussregel entfernen, werden die Änderungen sofort übernommen.

So entfernen Sie eine E-Mail-Flussregel

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Organization settings (Organisationseinstellungen) und Inbound/Outbound rules (Regeln für ein-/ausgehenden Datenverkehr) aus.
4. Wählen Sie die Regel und dann Remove aus.
5. Wählen Sie an der Bestätigungsaufforderung Remove (Entfernen) aus.

Durchsetzen von DMARC-Richtlinien für eingehende E-Mails

E-Mail-Domains verwenden aus Sicherheitsgründen DNS-Einträge (Domain Name System). Sie schützen Ihre Benutzer vor häufigen Angriffen wie Spoofing oder Phishing. DNS-Einträge enthalten häufig DMARC-Einträge (Domain-based Message Authentication, Reporting and Conformance), die vom Domaininhaber festgelegt werden, der die E-Mail sendet. DMARC-Einträge enthalten Richtlinien, die festlegen, welche Maßnahmen zu ergreifen sind, wenn eine E-Mail eine DMARC-Prüfung nicht besteht. Sie können wählen, ob die DMARC-Richtlinie für E-Mails durchgesetzt werden soll, die an Ihre Organisation gesendet werden.

Neue WorkMail Amazon-Organisationen haben die DMARC-Durchsetzung standardmäßig aktiviert.

Aktivieren der DMARC-Erzwingung

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Klicken Sie im Navigationsbereich auf Organization settings (Organisationseinstellungen). Die Seite mit den Organisationseinstellungen wird mit einer Reihe von Registerkarten angezeigt.
4. Wählen Sie die Registerkarte DMARC und dann Bearbeiten.
5. Stellen Sie den Schieberegler für die DMARC-Durchsetzung auf die Position Ein.
6. Aktivieren Sie das Kontrollkästchen neben Ich bestätige, dass die Aktivierung der DMARC-Durchsetzung dazu führen kann, dass eingehende E-Mails je nach Domainkonfiguration des Absenders gelöscht oder unter Quarantäne gestellt werden.
7. Wählen Sie Speichern.

Deaktivieren der DMARC-Durchsetzung

- Folgen Sie den Schritten im vorherigen Abschnitt, stellen Sie jedoch den Schieberegler für die DMARC-Durchsetzung auf Aus.

Verwenden der E-Mail-Ereignisprotokollierung zum Nachverfolgen der DMARC-Durchsetzung

Das Aktivieren der DMARC-Durchsetzung kann dazu führen, dass eingehende E-Mails gelöscht oder als Spam markiert werden, je nachdem, wie der Absender seine Domain konfiguriert hat. Wenn ein Absender seine E-Mail-Domain falsch konfiguriert, erhalten Ihre Benutzer ordnungsgemäße E-Mails möglicherweise nicht mehr. Um nach E-Mails zu suchen, die Ihren Benutzern nicht zugestellt wurden, können Sie die E-Mail-Ereignisprotokollierung für Ihre WorkMail Amazon-Organisation aktivieren. Anschließend können Sie Ihre E-Mail-Ereignisprotokolle nach eingehenden E-Mails abfragen, die basierend auf den DMARC-Richtlinien des Absenders herausgefiltert werden.

Bevor Sie die E-Mail-Ereignisprotokollierung verwenden, um die DMARC-Durchsetzung nachzuverfolgen, aktivieren Sie die E-Mail-Ereignisprotokollierung in der WorkMail Amazon-Konsole. Um Ihre Protokolldaten optimal zu nutzen, warten Sie, bis einige E-Mail-Ereignisse protokolliert wurden. Weitere Informationen und Anweisungen finden Sie unter the section called “Einschalten der E-Mail-Ereignisprotokollierung”.

Verwenden der E-Mail-Ereignisprotokollierung zur Nachverfolgung der DMARC-Durchsetzung

1. Wählen Sie in der CloudWatch Insights-Konsole unter Logs die Option Insights aus.
2. Wählen Sie unter Protokollgruppe (n) auswählen die Protokollgruppe Ihrer WorkMail Amazon-Organisation aus. Zum Beispiel/aws/workmail/events/organization-alias.
3. Wählen Sie einen abzufragenden Zeitraum aus.
4. Führen Sie die folgende Abfrage aus: stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. Wählen Sie Abfrage ausführen.

Sie können auch benutzerdefinierte Metriken für diese Ereignisse einrichten. Weitere Informationen finden Sie unter Erstellen von Metrikfiltern.

Markieren einer Organisation

Wenn Sie eine WorkMail Amazon-Organisationsressource taggen, können Sie:

- Unterscheiden Sie in der AWS Fakturierung und Kostenmanagement Konsole zwischen Organisationen.

- Steuern Sie den Zugriff auf WorkMail Amazon-Organisationsressourcen, indem Sie sie zu den `Resource` Element of AWS Identity and Access Management (IAM) - Berechtigungsrichtlinienerklärungen hinzufügen.

Weitere Informationen zu Amazon-Berechtigungen WorkMail auf Ressourcenebene finden Sie unter. Ressourcen Weitere Hinweise zum Steuern des Zugriffs auf der Grundlage von Tags finden Sie unter Autorisierung basierend auf WorkMail Amazon-Tags.

WorkMail Amazon-Administratoren können Organisationen mithilfe der WorkMail Amazon-Konsole taggen.

Um Stichwörter zu einer WorkMail Amazon-Organisation hinzuzufügen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie Tags aus.
4. Wählen Sie für Organization Tags (Organisation-Tags) die Option Add new tag (Neuen Tag hinzufügen).
5. Geben Sie unter Schlüssel einen Namen ein, der das Tag identifiziert.
6. (Optional) Geben Sie unter Value (Wert) einen Wert für den Tag ein.
7. (Optional) Wiederholen Sie die Schritte 4-6, um Ihrer Organisation weitere Tags hinzuzufügen. Sie können bis zu 50 Tags hinzufügen.
8. Wählen Sie Speichern, um Ihre Änderungen zu speichern.

Sie können Ihre Organisations-Tags in der WorkMail Amazon-Konsole einsehen.

Entwickler können Organisationen auch mithilfe des AWS SDK oder AWS Command Line Interface (AWS CLI) taggen. Weitere Informationen finden Sie in den `UntagResource` Befehlen `TagResourceListTagsForResource`, und in der Amazon WorkMail API-Referenz oder der AWS CLI Befehlsreferenz.

Sie können Tags jederzeit über die WorkMail Amazon-Konsole aus einer Organisation entfernen.

So entfernen Sie Tags aus einer WorkMail Amazon-Organisation

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie Tags aus.
4. Wählen Sie für Organization tags (Organisation-Tags) neben dem zu entfernenden Tag Remove (Entfernen).
5. Wählen Sie Submit (Absenden), um Ihre Änderungen zu speichern.

Arbeiten mit Zugriffssteuerungsregeln

Mit den Zugriffskontrollregeln für Amazon WorkMail können Administratoren steuern, wie Benutzern und Impersonationsrollen ihrer Organisation Zugriff auf Amazon gewährt wird. WorkMail Jede WorkMail Amazon-Organisation hat eine Standard-Zugriffskontrollregel, die allen Benutzern, die der Organisation hinzugefügt wurden, Postfachzugriff gewährt, und zwar unabhängig davon, welches Zugriffsprotokoll oder welche IP-Adresse sie verwenden. Administratoren können die Standardregel bearbeiten oder durch eine eigene ersetzen, eine neue Regel hinzufügen oder eine Regel löschen.

> **Warning**
>
> Wenn ein Administrator alle Zugriffskontrollregeln für eine Organisation löscht, WorkMail blockiert Amazon den gesamten Zugriff auf die Postfächer der Organisation.

Administratoren können Zugriffssteuerungsregeln anwenden, die den Zugriff basierend auf den folgenden Kriterien zulassen oder verweigern:

- Protokolle — Das Protokoll, das für den Zugriff auf das Postfach verwendet wird. Beispiele hierfür sind Autodiscover, EWS, IMAP, SMTP ActiveSync, Outlook für Windows und Webmail.
- IP-Adressen — Die IPv4 CIDR-Bereiche, die für den Zugriff auf das Postfach verwendet werden.
- WorkMail Amazon-Benutzer — Die Benutzer in Ihrer Organisation, die für den Zugriff auf das Postfach verwendet werden.

- Identitätswechselrollen — Die Identitätswechselrollen in Ihrer Organisation, die für den Zugriff auf das Postfach verwendet werden. Weitere Informationen finden Sie unter Verwaltung von Identitätswechselrollen.

Administratoren wenden Zugriffssteuerungsregeln zusätzlich zu den Postfach- und Ordnerberechtigungen des Benutzers an. Weitere Informationen finden Sie unter Ordner teilen Arbeiten mit Postfachberechtigungen und Ordnerberechtigungen im WorkMail Amazon-Benutzerhandbuch.

> **Note**
>
> - Wenn Sie den Zugriff für Outlook für Windows aktivieren, wird empfohlen, auch den Zugriff für Autodiscover und EWS zu aktivieren.
> - Die Regeln zur Zugriffskontrolle gelten nicht für den Zugriff auf die WorkMail Amazon-Konsole oder das SDK. Verwenden Sie stattdessen AWS Identity and Access Management (IAM) -Rollen oder -Richtlinien. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon WorkMail.

Erstellen von Zugriffssteuerungsregeln

Erstellen Sie neue Zugriffskontrollregeln von der WorkMail Amazon-Konsole aus.

So erstellen Sie eine neue Zugriffssteuerungsregel

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie Access control rules (Zugriffssteuerungsregeln) aus.
4. Wählen Sie Regel erstellen aus.
5. Geben Sie unter Description (Beschreibung) eine Beschreibung für die Regel ein.

6. Wählen Sie unter Effect (Auswirkung) die Option Allow (Zulassen) oder Deny (Verweigern) aus. Dies ermöglicht oder verweigert den Zugriff basierend auf den Bedingungen, die Sie im folgenden Schritt auswählen.
7. Denn Diese Regel gilt für Anfragen, die... , wählen Sie die Bedingungen aus, die für die Regel gelten sollen, z. B. ob bestimmte Protokolle, IP-Adressen oder Benutzer oder Identitätswechselrollen ein- oder ausgeschlossen werden sollen.
8. (Optional) Wenn Sie IP-Adressbereiche, Benutzer oder Identitätswechselrollen eingeben, wählen Sie Hinzufügen aus, um sie der Regel hinzuzufügen.
9. Wählen Sie Regel erstellen aus.

Bearbeiten von Zugriffssteuerungsregeln

Bearbeiten Sie neue und standardmäßige Zugriffskontrollregeln von der WorkMail Amazon-Konsole aus.

So bearbeiten Sie eine Zugriffssteuerungsregel

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie Access control rules (Zugriffssteuerungsregeln) aus.
4. Wählen Sie die zu bearbeitende Regel aus.
5. Wählen Sie Edit rule.
6. Bearbeiten Sie die Beschreibung, die Auswirkung und die Bedingungen nach Bedarf.
7. Wählen Sie Änderungen speichern aus.

> **Important**
>
> Wenn Sie eine Zugriffsregel ändern, kann es fünf Minuten dauern, bis die betroffenen Postfächer der aktualisierten Regel folgen. Clients, die auf die betroffenen Postfächer zugreifen, verhalten sich während dieser Zeit möglicherweise inkonsistent. Sie werden jedoch

sofort das richtige Verhalten feststellen, wenn Sie Ihre Regeln testen. Weitere Informationen zum Testen von Regeln finden Sie in den Schritten im nächsten Abschnitt.

Testen von Zugriffssteuerungsregeln

Um zu sehen, wie die Zugriffskontrollregeln Ihres Unternehmens angewendet werden, testen Sie die Regeln von der WorkMail Amazon-Konsole aus.

So testen Sie Zugriffssteuerungsregeln für Ihre Organisation

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie Access control rules (Zugriffssteuerungsregeln) aus.
4. Klicken Sie auf Test rules (Regeln testen).
5. Wählen Sie unter Request context (Anforderungskontext) das zu testende Protokoll aus.
6. Geben Sie unter Source IP address (Quell-IP-Adresse) die zu testende IP-Adresse ein.
7. Wählen Sie für „Anfrage ausgeführt von“ die Rolle „Benutzer“ oder „Identitätswechsel“ aus, für die Sie den Test durchführen möchten.
8. Wählen Sie die Rolle „Benutzer“ oder „Identitätswechsel“ aus, für die Sie den Test durchführen möchten.
9. Wählen Sie Test aus.

Die Testergebnisse werden unter Effect (Auswirkung) angezeigt.

Löschen von Zugriffssteuerungsregeln

Löschen Sie Zugriffskontrollregeln, die Sie nicht mehr benötigen, von der WorkMail Amazon-Konsole.

> **Warning**
>
> Wenn ein Administrator alle Zugriffskontrollregeln für eine Organisation löscht, WorkMail blockiert Amazon den gesamten Zugriff auf die Postfächer der Organisation.

So löschen Sie eine Zugriffssteuerungsregel

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie Access control rules (Zugriffssteuerungsregeln) aus.
4. Wählen Sie die zu löschende Regel aus.
5. Klicken Sie auf Delete rule (Regel löschen).
6. Wählen Sie Löschen aus.

Festlegen von Postfachaufbewahrungsrichtlinien

Sie können Richtlinien zur Aufbewahrung von Postfächern für Ihre WorkMail Amazon-Organisation festlegen. Aufbewahrungsrichtlinien löschen E-Mail-Nachrichten nach einem von Ihnen gewählten Zeitraum automatisch aus Benutzerpostfächern. Sie können wählen, auf welche Postfachordner Aufbewahrungsrichtlinien angewendet werden sollen. Sie können auch wählen, ob Sie unterschiedliche Aufbewahrungsrichtlinien für verschiedene Ordner festlegen möchten. Postfachaufbewahrungsrichtlinien gelten für die ausgewählten Ordner in allen Benutzerpostfächern in Ihrer Organisation. Benutzer können die Aufbewahrungsrichtlinien nicht außer Kraft setzen.

So legen Sie eine Postfachaufbewahrungsrichtlinie fest

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.

3. Wählen Sie Aufbewahrungsrichtlinie.
4. Wählen Sie unter Ordneraktionen neben jedem Postfachordner, den Sie in die Richtlinie aufnehmen möchten, die Option Löschen oder Dauerhaft löschen aus.
5. Geben Sie die Anzahl der Tage ein, für die die E-Mail-Nachrichten in den einzelnen Postfachordnern aufbewahrt werden sollen, bevor sie gelöscht werden.
6. Wählen Sie Speichern.

Warten Sie 48 Stunden, bis die Aufbewahrungsrichtlinien für Ihre Organisation angewendet werden. Wenn Sie die Aktion Ordner löschen wählen, können Benutzer gelöschte E-Mail-Nachrichten aus der WorkMail Amazon-Webanwendung und unterstützten Clients wiederherstellen. Wenn Sie die Aktion Ordner dauerhaft löschen wählen, können E-Mail-Nachrichten nicht wiederhergestellt werden, nachdem sie gelöscht wurden.

Die Anzahl der Tage, an denen ein Element in einer Aufbewahrungsrichtlinie aufbewahrt wird, hängt davon ab, wann es erstellt, geändert oder verschoben wurde. Wenn eine Aufbewahrungsrichtlinie beispielsweise Elemente nach einem Jahr löscht, zählt die Richtlinie die Aufbewahrungstage ab dem Datum, an dem Sie das Element erstellt oder zuletzt bearbeitet haben. Das Datum, an dem Sie die Aufbewahrungsrichtlinie eingeführt haben, hat keinen Einfluss darauf.

Arbeiten mit Domänen

Sie können Amazon WorkMail für die Verwendung einer benutzerdefinierten Domain konfigurieren. Sie können eine Domäne auch zur Standarddomäne für Ihre Organisation machen und sie AutoDiscover für Microsoft Outlook aktivieren.

Themen

- Hinzufügen einer Domäne
- Entfernen einer Domäne
- Auswählen der Standarddomäne
- Verifizieren von Domänen
- Aktivierung AutoDiscover zur Konfiguration von Endpunkten
- Bearbeiten von Domänenidentitätsrichtlinien
- Authentifizierung Ihrer E-Mails mit SPF
- Konfiguration einer benutzerdefinierten MAIL FROM-Domain

Hinzufügen einer Domäne

Sie können Ihrer WorkMail Amazon-Organisation bis zu 100 Domains hinzufügen. Wenn Sie eine neue Domain hinzufügen, wird der Domain-Identitätsrichtlinie automatisch eine Versandautorisierungsrichtlinie von Amazon Simple Email Service (Amazon SES) hinzugefügt. Dadurch hat Amazon WorkMail Zugriff auf alle Amazon SES SES-Sendeaktionen für Ihre Domain und Sie können E-Mails an Ihre Domain weiterleiten. Sie können E-Mails auch an externe Domains umleiten.

> **Note**
>
> Als bewährte Methode sollten Sie allen Ihren Domains Aliase für `<postmaster@>` und `<abuse@>` hinzufügen. Sie können Verteilergruppen für diese Aliase erstellen, wenn Sie möchten, dass bestimmte Benutzer in Ihrer Organisation E-Mails erhalten, die an diese Aliase gesendet werden.

Wenn Sie Ihre WorkMail Amazon-Organisation mit einer benutzerdefinierten Domain konfigurieren, sollten Sie Folgendes zu den DNS-Einträgen Ihrer Domain beachten:

- Für MX- und Autodiscover-CNAME-Einträge empfehlen wir, den Wert Time to Live (TTL) auf 3600 festzulegen. Durch die Reduzierung der TTL wird sichergestellt, dass Ihre Mailserver keine veralteten oder ungültigen MX-Einträge verwenden, nachdem Sie diese Einträge aktualisiert oder Ihre Postfächer migriert haben.
- Nachdem Sie Ihre Benutzer und Verteilergruppen erstellt und anschließend Ihre Postfächer erfolgreich migriert haben, sollten Sie den MX-Eintrag aktualisieren, um mit der Weiterleitung von E-Mails an Amazon WorkMail zu beginnen. Aktualisierungen von DNS-Datensätzen können bis zu 48 Stunden in Anspruch nehmen.
- Einige DNS-Anbieter hängen Domainnamen automatisch an die Enden der DNS-Einträge an. Das Hinzufügen eines Eintrags, der den Domainnamen bereits enthält, z. B. _amazonses.example.com, kann dazu führen, dass der Domainname dupliziert wird, was zu _amazonses.example.com.example.com führt. Fügen Sie im DNS-Datensatz einen Punkt an das Ende des Domänennamens an, um eine Duplizierung des Domänennamens im DNS-Datensatz zu vermeiden. Dies zeigt Ihrem DNS-Anbieter, dass der Datensatzname vollständig qualifiziert ist und nicht mehr mit dem Domainnamen verwandt ist. Darüber hinaus wird verhindert, dass der DNS-Anbieter einen zusätzlichen Domänennamen anfügt.
- Kopierte Datensatznamen enthalten den Domainnamen. Je nachdem, welchen DNS-Service-Anbieter Sie verwenden, wurde der Domänenname dem DNS-Datensatz der Domäne möglicherweise bereits hinzugefügt.
- Nachdem Sie einen DNS-Eintrag erstellt haben, wählen Sie das Aktualisierungssymbol auf der WorkMail Amazon-Konsole, um den Bestätigungsstatus und den Datensatzwert zu sehen. Weitere Informationen zum Verifizieren von Domänen finden Sie unter Verifizieren von Domänen.
- Wir empfehlen Ihnen, Ihre Domain als Domain zu `MAIL FROM` konfigurieren. Um sie AutoDiscover für iOS-Geräte zu aktivieren, müssen Sie Ihre Domain als `MAIL FROM` Domain konfigurieren. Sie können den Status Ihrer `MAIL FROM` Domain im Bereich „Zustellbarkeit verbessern“ der Konsole einsehen. Weitere Informationen finden Sie unter Konfiguration einer benutzerdefinierten MAIL FROM-Domain.

So fügen Sie eine Domäne hinzu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

2. Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
3. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, zu der Sie eine Domäne hinzufügen möchten.
4. Wählen Sie im Navigationsbereich Domänen und dann Domäne hinzufügen aus.
5. Geben Sie auf dem Bildschirm „Domain hinzufügen“ einen Domainnamen ein. Domainnamen dürfen nur lateinische Zeichen (ASCII) enthalten.

   > **Note**
   >
   > Wenn Sie eine Domain haben, die in einer öffentlich gehosteten Zone von Amazon Route 53 verwaltet wird, können Sie sie aus dem Drop-down-Menü auswählen, das bei der Eingabe eines Domainnamens angezeigt wird.

6. Wählen Sie Domain hinzufügen.

   Eine Seite wird angezeigt, auf der die DNS-Einträge für die neue Domain aufgelistet sind. Die Seite gruppiert die Einträge in die folgenden Abschnitte:

   - Besitz der Domain
   - WorkMail Konfiguration
   - Verbesserte Sicherheit
   - Verbesserte E-Mail-Zustellung

   Jeder dieser Abschnitte enthält einen oder mehrere DNS-Einträge, und jeder Datensatz zeigt einen Statuswert an. Die folgende Liste zeigt die Datensätze und ihre verfügbaren Statuswerte.

   TXT-Besitz

   Verifiziert — Datensatz gelöst und verifiziert.

   Ausstehend — Datensatz noch nicht verifiziert.

   Fehlgeschlagen — Die Inhaberschaft konnte nicht bestätigt werden. Datensatz nicht übereinstimmend oder nicht erreichbar.

WorkMail MX-Konfiguration

Verifiziert — Datensatz gelöst und verifiziert.

Fehlt — Datensatz konnte nicht aufgelöst werden.

Inkonsistent — Der Wert entspricht nicht dem erwarteten Datensatz.

AutoDiscover

Verifiziert — Datensatz aufgelöst und verifiziert.

Fehlt — Datensatz konnte nicht aufgelöst werden.

Inkonsistent — Der Wert entspricht nicht dem erwarteten Datensatz.

> **Note**
>
> Bei der AutoDiscover Überprüfung wird auch geprüft, ob die AutoDiscover Einrichtung korrekt ist. Der Prozess überprüft die Konfigurationseinstellungen für jede Phase. Wenn die Überprüfung abgeschlossen ist, erscheint in der Spalte Status ein grünes Häkchen neben Verifiziert. Sie können den Mauszeiger über Verifiziert bewegen und sehen, welche der Phasen durch den Prozess verifiziert wurde. Weitere Informationen zu den AutoDiscover Phasen finden Sie unterAktivierung AutoDiscover zur Konfiguration von Endpunkten.

DKIM CNAME

Verifiziert — Datensatz gelöst und verifiziert.

Ausstehend — Datensatz noch nicht verifiziert

Fehlgeschlagen — Die Inhaberschaft konnte nicht verifiziert werden. Datensatz nicht übereinstimmend oder nicht erreichbar.

Weitere Informationen zur DKIM-Signatur finden Sie unter Authentifizierung von E-Mails mit DKIM in Amazon SES im Amazon Simple Email Service Developer Guide.

SPF TXT

Verifiziert — Datensatz gelöst und verifiziert.

Fehlt — Datensatz konnte nicht aufgelöst werden.

Inkonsistent — Der Wert entspricht nicht dem erwarteten Datensatz.

Weitere Informationen zur SPF-Verifizierung finden Sie unter Authentifizierung Ihrer E-Mails mit SPF.

DMARC TXT

Verifiziert — Datensatz gelöst und verifiziert.

Fehlt — Datensatz konnte nicht aufgelöst werden.

Inkonsistent — Der Wert entspricht nicht dem erwarteten Datensatz

Weitere Informationen zu DMARC-Einträgen in Amazon WorkMail finden Sie unter Einhaltung von DMARC mithilfe von Amazon SES im Amazon Simple Email Service Developer Guide.

TXT-MAIL VON DER Domain

Verifiziert — Datensatz gelöst und verifiziert.

Ausstehend — Datensatz noch nicht verifiziert.

Fehlgeschlagen — Die Inhaberschaft konnte nicht bestätigt werden. Datensatz nicht übereinstimmend oder nicht erreichbar.

MX MAIL AUS der Domäne

Verifiziert — Datensatz gelöst und verifiziert.

Fehlt — Datensatz konnte nicht aufgelöst werden.

Inkonsistent — Der Wert entspricht nicht dem erwarteten Datensatz.

7. Wählen Sie für den nächsten Schritt die entsprechende Aktion aus, die auf dem von Ihnen verwendeten DNS-Anbieter basiert.

   Wenn Sie eine Route 53-Domain verwenden

   - Wählen Sie oben auf der Seite in Route 53 die Option Alle aktualisieren aus.

Wenn Sie einen anderen DNS-Anbieter verwenden

- Kopieren Sie die Datensätze und fügen Sie sie in Ihren DNS-Anbieter ein. Sie können die Datensätze in großen Mengen oder einzeln kopieren. Um Datensätze in großen Mengen zu kopieren, wählen Sie Alle kopieren aus. Dadurch wird eine Dateizone erstellt, die Sie in Ihren DNS-Anbieter importieren können. Um Datensätze einzeln zu kopieren, wählen Sie die überlappenden Quadrate neben dem Datensatznamen aus und fügen Sie sie dann jeweils in Ihren DNS-Anbieter ein.

8. Wählen Sie das Aktualisierungssymbol und aktualisieren Sie den Status für jeden Datensatz. Dadurch werden der Domainbesitz und die korrekte Konfiguration Ihrer Domain bei Amazon WorkMail überprüft.

Entfernen einer Domäne

Wenn Sie eine Domäne nicht mehr benötigen, können Sie sie löschen. Sie müssen jedoch zuerst alle Personen oder Gruppen löschen, die die Domain als E-Mail-Adresse verwenden.

So entfernen Sie eine Domäne

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Regionsname und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Aktivieren Sie in der Liste der Domänen das Kontrollkästchen neben dem Domänennamen und wählen Sie Remove aus.
4. Geben Sie im Dialogfeld Domäne entfernen den Namen der zu entfernenden Domäne ein und wählen Sie Entfernen aus.

Auswählen der Standarddomäne

Sie können eine mit Ihrer Organisation verknüpfte Domain zur Standarddomain für Benutzer und Gruppen in dieser Organisation machen. Wenn Sie eine Domäne als Standard festlegen, werden vorhandene E-Mail-Adressen nicht geändert.

So machen Sie eine Domäne zur Standarddomäne

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Regionsname und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Aktivieren Sie in der Liste der Domänen das Kontrollkästchen neben dem Domainnamen, den Sie verwenden möchten, und wählen Sie Als Standard festlegen aus.

Verifizieren von Domänen

Sie müssen Ihre Domain verifizieren, nachdem Sie sie in der WorkMail Amazon-Konsole hinzugefügt haben. Durch die Überprüfung der Domain wird bestätigt, dass Sie Eigentümer der Domain sind und Amazon WorkMail als E-Mail-Service für die Domain verwenden.

Sie verifizieren eine Domain, indem Sie ihr in Ihrem DNS-Dienst TXT- und MX-Einträge hinzufügen. Mit TXT-Einträgen können Sie Ihrem DNS-Dienst Notizen hinzufügen. MX-Einträge geben den Posteingangsserver an.

Sie verwenden die Amazon SES SES-Konsole, um die TXT- und MX-Einträge zu erstellen, und dann verwenden Sie die WorkMail Amazon-Konsole, um die Einträge zu Ihrem DNS-Service hinzuzufügen. Dazu gehen Sie wie folgt vor:

Um TXT- und MX-Einträge zu erstellen

1. Öffnen Sie die Amazon SES SES-Konsole unter https://console.aws.amazon.com/ses/.
2. Wählen Sie im Navigationsbereich Domains und anschließend Verify a New Domain aus.

   Das Dialogfeld „Neue Domäne verifizieren“ wird angezeigt.
3. Geben Sie im Feld Domäne den Namen der Domäne ein, die Sie in dem Hinzufügen einer Domäne Abschnitt erstellt haben.
4. (Optional) Wenn Sie DomainKeys Identified Mail (DKIM) verwenden möchten, aktivieren Sie das Kontrollkästchen DKIM-Einstellungen generieren.
5. Wählen Sie Verify this Domain aus.

Die Konsole zeigt eine Liste von TXT- und MX-Einträgen an.

6. Wählen Sie den Link Datensatz als CSV herunterladen, der sich unter der TXT-Liste befindet.

   Das Dialogfeld „Speichern unter“ wird angezeigt. Wählen Sie einen Speicherort für den Download und klicken Sie dann auf Speichern.

7. Öffnen Sie die heruntergeladene CSV-Datei und kopieren Sie ihren gesamten Inhalt.

Sobald Sie die TXT- und MX-Einträge erstellt haben, fügen Sie sie Ihrem DNS-Anbieter hinzu. Die folgenden Schritte verwenden Route 53. Wenn Sie einen anderen DNS-Anbieter verwenden und nicht wissen, wie man Datensätze hinzufügt, schlagen Sie in der Dokumentation Ihres Anbieters nach.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones. Wählen Sie dann das Optionsfeld neben der Domain aus, die Sie verifizieren möchten.
3. Wählen Sie aus der Liste der DNS-Einträge für Ihre Domain die Option Zonendatei importieren aus.
4. Fügen Sie unter Zonendatei die kopierten Datensätze in das Textfeld ein. Eine Liste der Dateien wird unter dem Textfeld angezeigt.
5. Scrollen Sie bis zum Ende der Liste und wählen Sie Import.

> **Note**
>
> Warten Sie bis zu 72 Stunden, um den Überprüfungsprozess abzuschließen.

Überprüfen von TXT-Datensätzen und MX-Datensätzen mit Ihrem DNS-Service

Vergewissern Sie sich, dass der TXT-Datensatz, der bestätigt, dass Sie Eigentümer der Domäne sind, korrekt zu Ihrem DNS-Service hinzugefügt wird. Dieses Verfahren verwendet das Tool nslookup, das für Windows und Linux verfügbar ist. Unter Linux können Sie auch dig verwenden.

Um das `nslookup` Tool verwenden zu können, müssen Sie zunächst die DNS-Server finden, die Ihre Domain bedienen. Anschließend fragen Sie diese Server ab, um die TXT-Einträge einzusehen. Sie können die DNS-Server für Ihre Domain abfragen, da diese Server die meisten up-to-date Informationen für Ihre Domain enthalten. Es kann einige Zeit dauern, bis diese Informationen von anderen DNS-Servern übernommen werden.

Verwenden Sie nslookup, um zu überprüfen, ob Ihr TXT-Eintrag zu Ihrem DNS-Dienst hinzugefügt wurde

1. Finden Sie die Nameserver Ihrer Domain:

   a. Öffnen Sie eine Befehlszeile (Windows) oder ein Terminal (Linux).

   b. Führen Sie den folgenden Befehl aus, um alle Nameserver aufzulisten, die Ihre Domain bedienen. Ersetze es *`example.com`* durch deine Domain.

   ```
   nslookup -type=NS example.com
   ```

   Im nächsten Schritt fragen Sie einen dieser Nameserver ab.

2. Stellen Sie sicher, dass der Amazon WorkMail TXT-Eintrag korrekt hinzugefügt wurde.

   a. Führen Sie den folgenden Befehl aus und *`example.com`* ersetzen Sie ihn durch Ihre Domain und *`ns1.name-server.net`* durch einen Nameserver aus Schritt 1.

   ```
   nslookup -type=TXT _amazonses.example.com ns1.name-server.net
   ```

   b. Überprüfen Sie die `"text ="` Zeichenfolge, die in der Ausgabe von angezeigt wirdnslookup. Vergewissern Sie sich, dass diese Zeichenfolge mit dem TXT-Wert für Ihre Domain in der Liste der verifizierten Absender in der WorkMail Amazon-Konsole übereinstimmt.

   Im folgenden Beispiel möchten Sie einen TXT-Eintrag für _amazonses.example.com mit einem Wert von sehen. `fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk=` Wenn Sie den Datensatz korrekt aktualisieren, hat der Befehl die folgende Ausgabe:

   ```
   _amazonses.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
   ```

Verwenden Sie dig, um zu überprüfen, ob Ihr TXT-Eintrag zu Ihrem DNS-Dienst hinzugefügt wurde

1. Öffnen Sie eine Terminalsitzung.
2. Führen Sie den folgenden Befehl aus, um die TXT-Einträge für Ihre Domain aufzulisten. Ersetze es *example.com* durch deine Domain.

   ```
   dig +short example.com txt
   ```

3. Stellen Sie sicher, dass die Zeichenfolge, die TXT in der Befehlsausgabe folgt, mit dem TXT-Wert übereinstimmt, den Sie sehen, wenn Sie die Domain in der Liste der verifizierten Absender der WorkMail Amazon-Konsole auswählen.

So verwenden Sie nslookup, um zu überprüfen, ob Ihr MX-Datensatz zu Ihrem DNS-Service hinzugefügt wurde

1. Suchen Sie die Namensserver für Ihre Domäne:

   a. Öffnen Sie eine Befehlszeile.

   b. Führen Sie den folgenden Befehl aus, um alle Nameserver für Ihre Domain aufzulisten.

      ```
      nslookup -type=NS example.com
      ```

      Im nächsten Schritt fragen Sie einen dieser Nameserver ab.

2. Überprüfen Sie, ob der MX-Datensatz korrekt hinzugefügt wurde:

   a. Führen Sie den folgenden Befehl aus und *example.com* ersetzen Sie ihn durch Ihre Domain und *ns1.name-server.net* durch einen der Nameserver, die Sie im vorherigen Schritt identifiziert haben.

      ```
      nslookup -type=MX example.com ns1.name-server.net
      ```

   b. Vergewissern Sie sich bei der Ausgabe des Befehls, dass die auf `mail exchange =` folgende Zeichenfolge mit einem der folgenden Werte übereinstimmt:

      Region USA Ost (Nord-Virginia) — `10 inbound-smtp.us-east-1.amazonaws.com`

      Region USA West (Oregon) — `10 inbound-smtp.us-west-2.amazonaws.com`

      Region Europa (Irland) — `10 inbound-smtp.eu-west-1.amazonaws.com`

> **Note**
>
> `10` stellt die MX-Rangnummer oder -Priorität dar.

Verwenden Sie dig, um zu überprüfen, ob Ihr MX-Eintrag zu Ihrem DNS-Dienst hinzugefügt wurde

1. Öffnen Sie eine Terminalsitzung.
2. Führen Sie den folgenden Befehl aus, um die MX-Einträge für Ihre Domain aufzulisten.

```
dig +short example.com mx
```

3. Stellen Sie sicher, dass die Zeichenfolge nach `MX` mit einem der folgenden Werte übereinstimmt:

   Region USA Ost (Nord-Virginia) — `10 inbound-smtp.us-east-1.amazonaws.com`

   Region USA West (Oregon) — `10 inbound-smtp.us-west-2.amazonaws.com`

   Region Europa (Irland) — `10 inbound-smtp.eu-west-1.amazonaws.com`

   > **Note**
   >
   > `10` stellt die MX-Rangnummer oder -Priorität dar.

Fehlerbehebung bei der Domänenverifizierung

Sehen Sie sich die folgenden Vorschläge an, um häufig auftretende Probleme bei der Domainverifizierung zu beheben:

Ihr DNS-Dienst erlaubt keine Unterstriche in TXT-Eintragsnamen

Lassen Sie `_amazonses` den Namen des TXT-Eintrags weg.

Sie möchten dieselbe Domain mehrmals verifizieren, können aber nicht mehrere TXT-Einträge mit demselben Namen haben

Wenn Ihr DNS-Dienst nicht zulässt, dass Sie mehrere TXT-Einträge mit demselben Namen haben, verwenden Sie eine der folgenden Problemumgehungen:

- (Empfohlen) Wenn Ihr DNS-Dienst dies zulässt, weisen Sie dem TXT-Eintrag mehrere Werte zu. Wenn Ihr DNS beispielsweise von Amazon Route 53 verwaltet wird, können Sie mehrere Werte für denselben TXT-Eintrag wie folgt einrichten:
  1. Wählen Sie in der Route 53-Konsole den `_amazonses` TXT-Eintrag aus, den Sie hinzugefügt haben, als Sie Ihre Domain in der ersten Region verifiziert haben.
  2. Bei Value (Wert) drücken Sie nach dem ersten Wert die Enter (Eingabetaste).
  3. Fügen Sie den Wert für die zusätzlichen Region hinzu und speichern Sie den Datensatz.
- Wenn Sie Ihre Domain nur zweimal verifizieren müssen, können Sie sie einmal verifizieren, indem Sie einen TXT-Eintrag mit `_amazonses` im Namen und dann einen weiteren Eintrag ohne Eintrag `_amazonses` im Datensatznamen erstellen.

Die WorkMail Amazon-Konsole meldet, dass die Domainverifizierung fehlgeschlagen ist

Amazon WorkMail kann den erforderlichen TXT-Eintrag für Ihren DNS-Service nicht finden. Stellen Sie sicher, dass der erforderliche TXT-Eintrag korrekt zu Ihrem DNS-Dienst hinzugefügt wurde, indem Sie das Verfahren unter befolgenÜberprüfen von TXT-Datensätzen und MX-Datensätzen mit Ihrem DNS-Service.

Ihr DNS-Anbieter hat den Domainnamen an das Ende des TXT-Eintrags angehängt

Das Hinzufügen eines TXT-Eintrags, der den Domainnamen bereits enthält, z. B. _amazonses.example.com, kann dazu führen, dass der Domainname dupliziert wird, z. B. _amazonses.example.com.example.com. Fügen Sie am Ende des Domänenname im TXT-Datensatz einen Punkt hinzu, um die Duplizierung des Domänennamens im Datensatznamen zu vermeiden. Dies zeigt Ihrem DNS-Anbieter, dass der Eintragsname vollständig qualifiziert ist und der Domainname bereits im TXT-Eintrag enthalten ist.

Amazon WorkMail meldet, dass der MX-Datensatz inkonsistent ist

Bei der Migration von vorhandenen Mailservern gibt der MX-Eintrag möglicherweise den Status Inkonsistent zurück. Aktualisieren Sie Ihren MX-Eintrag so, dass er auf Amazon verweist, WorkMail anstatt auf Ihren vorherigen Mail-Server zu verweisen. Der MX-Eintrag wird auch als inkonsistent zurückgegeben, wenn ein E-Mail-Proxy eines Drittanbieters zusammen mit Amazon WorkMail verwendet wird. Wenn dies der Fall ist, kann die Inconsistent (Inkonsistent)-Warnung ignoriert werden.

Aktivierung AutoDiscover zur Konfiguration von Endpunkten

AutoDiscover ermöglicht es Ihnen, Microsoft Outlook und mobile Clients zu konfigurieren, indem Sie nur Ihre E-Mail-Adresse und Ihr Passwort verwenden. Der Service hält eine Verbindung zu Amazon aufrecht WorkMail und aktualisiert die lokalen Einstellungen, wenn Sie Endpunkte oder Einstellungen ändern. Darüber hinaus AutoDiscover kann Ihr Kunde zusätzliche WorkMail Amazon-Funktionen nutzen, z. B. das Offline-Adressbuch, den Out-of-Office Assistenten und die Möglichkeit, freie/gebuchte Zeiten im Kalender anzuzeigen.

Der Client führt die folgenden AutoDiscover Phasen durch, um den Serverendpunkt zu erkennen: URLs

- Phase 1 — Der Client führt eine SCP-Suche (Secure Copy Protocol) im lokalen Active Directory durch. Wenn Ihr Client nicht in die Domäne eingebunden ist, AutoDiscover überspringen Sie diesen Schritt.
- Phase 2 — Der Client sendet eine Anfrage an die folgende Stelle URLs und validiert die Ergebnisse. Diese Endpunkte sind nur über HTTPS verfügbar.
  - https:///autodiscover/autodiscover.xml *`company.tld`*
  - https://autodiscover. *`company.tld`*/autodiscover/autodiscover.xml
- Phase 3 — Der Client führt eine DNS-Suche nach autodiscover.company.tld durch und sendet von der E-Mail-Adresse des Benutzers aus eine nicht authentifizierte GET-Anfrage an den abgeleiteten Endpunkt. Wenn der Server eine 302-Umleitung zurückgibt, sendet der Client die Anfrage erneut an den zurückgegebenen HTTPS-Endpunkt. AutoDiscover

Wenn alle diese Phasen fehlschlagen, kann der Client nicht automatisch konfiguriert werden. Informationen zur manuellen Konfiguration von Endgeräten finden Sie unter Manuelles Verknüpfen mit dem Mobilgerät.

Sie werden aufgefordert, den AutoDiscover DNS-Eintrag zu Ihrem Anbieter hinzuzufügen, wenn Sie Ihre Domain zu Amazon hinzufügen WorkMail. Dadurch kann der Kunde Phase 3 des AutoDiscover Prozesses durchführen. Diese Schritte funktionieren jedoch nicht für alle Mobilgeräte, z. B. für die Standard-Android-E-Mail-App. Daher müssen Sie AutoDiscover Phase 2 möglicherweise manuell einrichten.

Sie können die folgenden Methoden verwenden, um AutoDiscover Phase 2 für Ihre Domain einzurichten:

(Empfohlen) Verwenden Sie Route 53 und Amazon CloudFront

> **Note**
>
> In den folgenden Schritten wird erklärt, wie Sie einen Proxy für https://autodiscover erstellen. *company.tld*/autodiscover/autodiscover.xml. Um einen Proxy für https://*company.tld*/autodiscover/autodiscover.xml zu erstellen, entfernen Sie in den folgenden Schritten das `autodiscover.` Präfix aus den Domänen.
> Für die Nutzung CloudFront und Route 53 können Gebühren anfallen. Weitere Informationen zu den geltenden Preisen finden Sie unter CloudFront Amazon-Preise und Amazon Route 53-Preise.

Um AutoDiscover Phase 2 mit Route 53 zu aktivieren und CloudFront

1. Besorgen Sie sich ein SSL-Zertifikat für Autodiscover. *company.tld*und lade es auf AWS Identity and Access Management (IAM) hoch oder. AWS Certificate Manager Weitere Informationen finden Sie unter Arbeiten mit Serverzertifikaten im IAM-Benutzerhandbuch oder Erste Schritte im AWS Certificate Manager Benutzerhandbuch.
2. Erstellen Sie eine neue CloudFront Distribution:
    1. Öffnen Sie die CloudFront Konsole unterhttps://console.aws.amazon.com/cloudfront/v4/home.
    2. Rufen Sie im Navigationsbereich Distributions auf.
    3. Wählen Sie Create Distribution (Distribution erstellen).
    4. Wählen Sie unter Web die Option Get Started aus.
    5. Geben Sie in den Origin-Einstellungen die folgenden Werte ein:
        - Origin-Domainname — Der passende Domainname für deine Region:
            - USA Ost (Nord-Virginia) — **`autodiscover-service.mail.us-east-1.awsapps.com`**
            - USA West (Oregon) — **`autodiscover-service.mail.us-west-2.awsapps.com`**
            - Europa (Irland) — **`autodiscover-service.mail.eu-west-1.awsapps.com`**
        - Politik des Ursprungsprotokolls — Die gewünschte Richtlinie: **`Match Viewer`**

> **Note**
>
> Lassen Sie den Origin-Pfad leer. Ändern Sie nicht den automatisch ausgefüllten Wert für Origin ID.

6. Wählen Sie in den Standardeinstellungen für das Cache-Verhalten die folgenden Werte für die aufgelisteten Einstellungen aus:
   - Viewer Protocol Policy (Viewerprotokollrichtlinie): HTTPS Only
   - Allowed HTTP Methods: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - Cache Based on Selected Request Headers (Cache basierend auf ausgewählte Anforderungsheader): Alle
   - Forward Cookies (Cookies weiterleiten): All
   - Query String Forwarding and Caching (Abfragezeichenfolgen-Weiterleitung und -Caching): Kein (verbessert das Caching)
   - Smooth Streaming: Nein
   - Restrict Viewer Access (Viewer-Zugriff einschränken): Nein
7. Wählen Sie die folgenden Werte für Distribution Settings (Verteilungseinstellungen):
   - Price Class (Preisklasse): Nur USA, Kanada und Europa verwenden
   - Geben Sie für Alternative Domainnamen (CNAMEs) **`autodiscover.`*`company.tld`*** oder ein***`company.tld`***, wo *`company.tld`* ist Ihr Domainname.
   - SSL-Zertifikat: Benutzerdefiniertes SSL-Zertifikat (in IAM gespeichert)
   - Custom SSL Client Support (Benutzerdefinierte SSL-Client-Unterstützung): Wählen Sie All Clients (Alle Clients) oder Only Clients that Support Server Name Indication (SNI) (Nur Clients, die Server Name Indication (Servernamensanzeige, SNI) unterstützen). Ältere Versionen von Android funktioniert möglicherweise nicht mit der letzteren Option.

     > **Note**
     >
     > Lassen Sie bei Wahl von All Clients (Alle Clients) das Feld Default Root Object (Standardstammobjekt) leer.

   - Logging (Protokollierung): Wählen Sie On (Ein) oder Off (Aus). On aktiviert die Protokollierung.

- Geben Sie unter Comment (Kommentar) **`AutoDiscover type2 for autodiscover.`*`company.tld`*** ein
- Verteilungsstatus: Wählen Sie Aktiviert.

8. Wählen Sie Create Distribution (Distribution erstellen).

3. Erstellen Sie in der Route 53-Konsole einen Eintrag, der den Internetverkehr für Ihren Domainnamen an Ihre CloudFront Distribution weiterleitet.

> **Note**
>
> Bei diesen Schritten wird davon ausgegangen, dass der DNS-Eintrag für example.com auf Route 53 gehostet wird. Wenn Sie Route 53 nicht verwenden, folgen Sie den Anweisungen in der Verwaltungskonsole Ihres DNS-Anbieters.

1. Wählen Sie im Navigationsbereich der Konsole Hosted Zones aus. Wählen Sie dann eine Domain aus.
2. Wählen Sie in der Liste der Domänen den Domainnamen aus, den Sie verwenden möchten.
3. Wählen Sie unter Datensätze die Option Datensatz erstellen aus.
4. Stellen Sie unter Datensatz schnell erstellen die folgenden Parameter ein:
   - Geben Sie unter Datensatzname einen Namen für den Datensatz ein.
   - Wählen Sie unter Routing-Richtlinie die Option Einfaches Routing aus.
   - Wählen Sie den Alias-Schieberegler, um ihn zu aktivieren. Der Schieberegler wird blau, wenn er eingeschaltet ist.
   - Wählen Sie in der Liste Datensatztyp die Option A — Leitet den Datenverkehr an eine IPv4 Adresse und einige AWS-Ressourcen weiter.
   - Wählen Sie in der Liste Traffic weiterleiten an die Option Alias to CloudFront Distribution aus.
   - Unter der Liste Traffic weiterleiten an wird ein Suchfeld angezeigt. Geben Sie den Namen Ihrer CloudFront Distribution in das Textfeld ein. Sie können Ihren Vertrieb auch aus der Liste auswählen, die angezeigt wird, wenn Sie das Suchfeld auswählen.
5. Wählen Sie Datensatz erstellen.

Verwenden Sie einen Apache-Webserver

In den folgenden Schritten wird erklärt, wie Sie einen Apache-Webserver verwenden, um einen Proxy für https://autodiscover zu erstellen. *company.tld*/autodiscover/autodiscover.xml. Um einen Proxy für https://*company.tld*/autodiscover/autodiscover.xml zu erstellen, entfernen Sie „Autodiscover“. Präfix aus den Domänen in den folgenden Schritten.

Um AutoDiscover Phase 2 mit einem Apache-Webserver zu aktivieren

1. Führen Sie die folgenden Anweisungen auf einem SSL-fähigen Apache-Server aus:

   ```
   SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-
   service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
   ```

2. Aktivieren Sie bei Bedarf die folgenden Apache-Module. Wenn Sie nicht wissen, wie das geht, lesen Sie in der Apache-Hilfe nach:

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`
   - `ssl`

Im folgenden Abschnitt finden Sie Informationen zum Testen und zur Fehlerbehebung AutoDiscover.

AutoDiscover Phase 2: Fehlerbehebung

Sobald Sie Ihren DNS-Anbieter für konfiguriert haben AutoDiscover, können Sie Ihre AutoDiscover Endpunktkonfiguration testen. Wenn Sie Ihren Endpunkt korrekt konfiguriert haben, antwortet er mit einer unautorisierten Anforderungsnachricht.

So führen Sie eine grundlegende unbefugte Anforderung durch

1. Erstellen Sie von einem Terminal aus eine nicht authentifizierte POST-Anfrage an den AutoDiscover Endpunkt.

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ```

Wenn Ihr Endpunkt korrekt konfiguriert ist, sollte er eine `401 unauthorized` Nachricht zurückgeben, wie im folgenden Beispiel gezeigt:

```
$ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
autodiscover.xml
...
HTTP/1.1 401 Unauthorized
```

2. Testen Sie als Nächstes eine echte AutoDiscover Anfrage. Erstellen Sie eine `request.xml` Datei mit dem folgenden XML-Inhalt:

```
<?xml version="1.0" encoding="utf-8"?>

<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
requestschema/2006">
    <Request>
        <EMailAddress>testuser@company.tld</EMailAddress>
        <AcceptableResponseSchema>
            http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006
        </AcceptableResponseSchema>
    </Request>
</Autodiscover>
```

3. Verwenden Sie die `request.xml` Datei, die Sie erstellt haben, und senden Sie eine authentifizierte AutoDiscover Anfrage an den Endpunkt. Denken Sie daran, es *`testuser@company.tld`* durch eine gültige E-Mail-Adresse zu ersetzen:

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

Die Antwort sieht ähnlich wie im folgenden Beispiel aus, wenn der Endpunkt korrekt konfiguriert ist:

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml

Enter host password for user 'testuser@company.tld':
<?xml version="1.0" encoding="UTF-8"?>
```

```
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/
responseschema/2006" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006">
    <Culture>en:us</Culture>
    <User>
        <DisplayName>User1</DisplayName>
        <EMailAddress>testuser@company.tld</EMailAddress>
    </User>
    <Action>
        <Settings>
            <Server>
                <Type>MobileSync</Type>
                <Url>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Url>
                <Name>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Name>
            </Server>
        </Settings>
    </Action>
</Response>
```

Bearbeiten von Domänenidentitätsrichtlinien

Domänenidentitätsrichtlinien spezifizieren Berechtigungen für E-Mail-Aktionen, wie z. B. das Umleiten von E-Mail-Nachrichten. Sie können beispielsweise E-Mails an jede E-Mail-Adresse in Ihrer WorkMail Amazon-Organisation weiterleiten.

> **Note**
>
> Ab dem 1. April 2022 WorkMail begann Amazon, Service Principals für die Autorisierung anstelle von AWS Account Principals zu verwenden. Wenn Sie vor dem 1. April 2022 eine Domain hinzugefügt haben, haben Sie möglicherweise eine ältere Richtlinie, die einen AWS Kontoprinzipal für die Autorisierung verwendet. In diesem Fall empfehlen wir, auf die neueste Richtlinie zu aktualisieren. In den Schritten in diesem Abschnitt wird erklärt, wie das geht. Ihr Unternehmen versendet während des Updates weiterhin normal E-Mails.

Sie befolgen diese Schritte nur, wenn Sie keine benutzerdefinierte Amazon SES SES-Richtlinie verwenden. Wenn Sie eine benutzerdefinierte Amazon SES SES-Richtlinie verwenden, müssen Sie diese selbst aktualisieren. Weitere Informationen finden Sie Benutzerdefinierte Amazon SES SES-Serviceprinzipalrichtlinie weiter unten in diesem Thema.

> **Important**
>
> Entfernen Sie Ihre vorhandenen Domains nicht. Wenn Sie das tun, unterbrechen Sie den E-Mail-Dienst. Sie müssen lediglich Ihre bestehenden Domains erneut eingeben.

Um eine Domain-Identitätsrichtlinie zu aktualisieren

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie dazu die Liste Region auswählen, die sich rechts neben dem Suchfeld befindet, und wählen Sie dann die gewünschte Region aus. Weitere Informationen zu Regionen finden Sie unter Regionen und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Domains aus.
4. Markieren und kopieren Sie den Namen der Domäne, die Sie erneut eingeben möchten, und wählen Sie dann Domäne hinzufügen aus.

   Das Dialogfeld „Domäne hinzufügen“ wird angezeigt.
5. Fügen Sie den kopierten Namen in das Feld Domainname ein und wählen Sie dann Domäne hinzufügen aus.
6. Wiederholen Sie die Schritte 3 bis 5 für die übrigen Domains in Ihrer Organisation.

Benutzerdefinierte Amazon SES SES-Serviceprinzipalrichtlinie

Wenn Sie eine benutzerdefinierte Amazon SES SES-Richtlinie verwenden, passen Sie dieses Beispiel für die Verwendung in Ihrer Domain an.

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

```
    {
      "Sid": "AuthorizeWorkMail",
      "Effect": "Allow",
      "Principal": {
        "Service": "workmail.REGION.amazonaws.com"
      },
      "Action": [
        "ses:*"
      ],
      "Resource": "arn:aws:ses:REGION:AWS_ACCOUNT_ID:identity/WORKMAIL-DOMAIN-NAME",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn":
 "arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID"
        }
      }
    }
  ]
}
```

Authentifizierung Ihrer E-Mails mit SPF

Das Sender Policy Framework (SPF) ist ein E-Mail-Validierungsstandard zur Bekämpfung von E-Mail-Spoofing. Beim Spoofing wird eine von einem böswilligen Akteur gesendete E-Mail so aussehen, als ob sie von einem legitimen Benutzer gesendet wurde. Informationen zur Konfiguration von SPF für Ihre WorkMail Amazon-fähige Domain finden Sie unter E-Mail-Authentifizierung mit SPF in Amazon SES.

Konfiguration einer benutzerdefinierten MAIL FROM-Domain

Standardmäßig WorkMail verwendet Amazon eine Subdomain von amazonses.com als `MAIL FROM` Domain für Ihre ausgehenden E-Mails. Dies kann dazu führen, dass die Zustellung fehlschlägt, wenn die DMARC-Richtlinie auf Ihrer Domain nur für SPF eingerichtet ist. Um dieses Problem zu beheben, konfigurieren Sie Ihre eigene Domain als Domain. `MAIL FROM` Informationen zum Einrichten Ihrer E-Mail-Domain als Domain finden Sie unter Einrichten einer benutzerdefinierten MAIL FROM-Domain im Amazon Simple Email Service Developer Guide. `MAIL FROM`

> **Important**
>
> Eine benutzerdefinierte MAIL FROM-Domäne ist erforderlich, wenn Sie sie AutoDiscover für iOS-Geräte aktivieren.

Weitere Informationen zu benutzerdefinierten `MAIL FROM` Domänen finden Sie unter Amazon SES unterstützt jetzt benutzerdefinierte MAIL FROM-Domänen.

Working with users

Sie können Benutzer bei Amazon erstellen und entfernen WorkMail. Darüber hinaus können Sie ihre E-Mail-Passwörter zurücksetzen, ihre Postfachkontingente und ihren Gerätezugriff verwalten und ihre Postfachberechtigungen kontrollieren.

Themen

- Eine Benutzerliste anzeigen
- Hinzufügen eines Benutzers
- Aktivieren von Benutzern
- Benutzer-Aliase verwalten
- Deaktivieren von Benutzern
- Editing user details
- Das Benutzerkennwort wird zurückgesetzt
- Fehlerbehebung bei WorkMail Amazon-Passwortrichtlinien
- Working with notifications
- Enabling signed or encrypted email

Eine Benutzerliste anzeigen

Um die Liste der Benutzer einzusehen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Klicken Sie im Navigationsbereich auf Users (Benutzer).
4. Darüber hinaus können Sie Benutzer nach Benutzername, Anzeigename oder primärer E-Mail-Adresse filtern.

> **Note**
>
> Bei der Suche wird Groß- und Kleinschreibung beachtet.

Hinzufügen eines Benutzers

Wenn Sie einen Benutzer hinzufügen, erstellt Amazon WorkMail automatisch Postfächer für ihn. Benutzer können sich über die WorkMail Amazon-Webanwendung, ihr Mobilgerät oder mithilfe von Microsoft Outlook auf macOS oder PC anmelden und auf ihre E-Mails zugreifen.

So fügen Sie einen Benutzer hinzu

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann die Organisation aus, zu der Sie Benutzer hinzufügen möchten.
3. Wählen Sie im Navigationsbereich Benutzer und dann Benutzer hinzufügen aus.

   Der Bildschirm Benutzer hinzufügen wird angezeigt.
4. Geben Sie unter Benutzerdetails im Feld Benutzername den Namen des Benutzers ein. Der Name wird auch im Feld E-Mail-Adresse angezeigt. Wenn Sie möchten, dass der Benutzer eine andere E-Mail-Adresse als sein Benutzername hat, können Sie das Feld E-Mail-Adresse bearbeiten.
5. (Optional) Geben Sie den Vor- und Nachnamen des Benutzers in die Felder Vorname und Nachname ein.
6. Geben Sie im Feld Anzeigename den Anzeigenamen des Benutzers ein.
7. Akzeptieren Sie im Feld E-Mail-Adresse den E-Mail-Alias oder geben Sie einen anderen ein.
8. Standardmäßig werden Benutzer in der globalen Adressliste angezeigt. Um den Benutzer aus der globalen Adressliste auszublenden, deaktivieren Sie das Kontrollkästchen In globaler Adressliste anzeigen.
9. Wählen Sie Kein Postfach erstellen aus, um der Organisation einen Benutzer als Remotebenutzer hinzuzufügen.

10. Geben Sie unter Passwortkonfiguration das Passwort des Benutzers in die Felder Passwort und Passwort wiederholen ein.
11. Wählen Sie Benutzer hinzufügen.

Aktivieren von Benutzern

Wenn Sie Amazon WorkMail in das Active Directory Ihres Unternehmens integrieren oder wenn Sie bereits Benutzer in Ihrem Simple AD AD-Verzeichnis verfügbar haben, können Sie diese Benutzer in Amazon aktivieren WorkMail. Sie gehen auch wie folgt vor, um einen Benutzer, dessen Konto deaktiviert wurde, erneut zu aktivieren.

So aktivieren Sie Benutzer

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann die Organisation aus, für die Sie Benutzer aktivieren möchten.
3. Klicken Sie im Navigationsbereich auf Users (Benutzer).

   Eine Liste von Benutzern wird angezeigt. Benutzerkonten im Benutzerstatus aktiviert, deaktiviert und Systembenutzer werden in der Liste angezeigt.
4. Wählen Sie in der Liste der Benutzer mit deaktivierten Konten die Kontrollkästchen für die Benutzer aus, die Sie aktivieren möchten, und wählen Sie dann Aktivieren aus.

   Das Dialogfeld „Benutzer aktivieren“ wird angezeigt.
5. Überprüfen und ändern Sie bei Bedarf die primäre E-Mail-Adresse für jeden Benutzer und wählen Sie dann Aktivieren aus.

Benutzer-Aliase verwalten

Sie können E-Mail-Aliase für Benutzer hinzufügen oder entfernen.

Um einem Benutzer einen E-Mail-Alias hinzuzufügen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, für die Sie Benutzer hinzufügen möchten.
3. Wählen Sie im Navigationsbereich Benutzer und dann den Namen des Benutzers aus, dem Sie einen Alias hinzufügen möchten.
4. Wählen Sie im Abschnitt Benutzerdetails die Registerkarte Aliase aus.
5. Wählen Sie auf der Registerkarte Aliase die Option Alias hinzufügen aus.
6. Geben Sie im Feld Alias einen Alias ein.
7. Wählen Sie eine Domain für einen Alias aus.
8. Wählen Sie Hinzufügen aus.

Um einen E-Mail-Alias von einem Benutzer zu entfernen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, aus der Sie Benutzer entfernen möchten.
3. Wählen Sie im Navigationsbereich Benutzer und dann den Namen des Benutzers aus, von dem Sie Aliase entfernen möchten.
4. Wählen Sie im Abschnitt Benutzerdetails die Registerkarte Aliase aus.
5. Aktivieren Sie auf der Registerkarte Aliase das Kontrollkästchen für die Aliase, die Sie entfernen möchten.
6. Überprüfen Sie die Aliase, die entfernt werden sollen.
7. Wählen Sie im Fenster Aliase entfernen die Option Entfernen aus.

Deaktivieren von Benutzern

Sie können jeden Benutzer in einer Organisation jederzeit deaktivieren. Wenn Sie einen Benutzer deaktivieren, kann sofort nicht mehr darauf zugegriffen werden. Bei Benutzern, die länger als 30 Tage deaktiviert sind, wird ihr Posteingang von Amazon gelöscht WorkMail.

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann die Organisation aus, die die Benutzer enthält, die Sie deaktivieren möchten.
3. Klicken Sie im Navigationsbereich auf Users (Benutzer).

   Es wird eine Liste aller Benutzer mit Konten angezeigt, die sich im Status „Aktiviert“, „Deaktiviert“ und „Systembenutzer“ befinden.
4. Wählen Sie in der Liste der aktivierten Benutzer die Kontrollkästchen für die Konten aus, die Sie deaktivieren möchten, und wählen Sie dann Deaktivieren aus.

   Das Dialogfeld „Benutzer deaktivieren“ wird angezeigt.
5. Wählen Sie Disable (deaktivieren) aus.

Editing user details

Wenn Sie die Benutzerdetails bearbeiten, können Sie Folgendes ändern:

- Persönliche Daten — Namen, E-Mail-Adressen, Telefonnummern und andere persönliche Daten.
- Postfachkontingente (Größen) — Kontingente können zwischen 1 MB und 51.200 MB (50 GB) liegen. Amazon WorkMail benachrichtigt Benutzer, wenn sie 90 Prozent ihrer Quote erreicht haben. Außerdem hat die Änderung des Postfachkontingents eines Benutzers keinen Einfluss auf die Preisgestaltung. Weitere Informationen zur Preisgestaltung finden Sie unter WorkMail Amazon-Preise.
- Zugriff auf mobile Geräte — Geräte entfernen und löschen und Gerätedetails anzeigen.
- Postfachzugriffsberechtigungen — Erteilen Sie Benutzern die Erlaubnis, ein Postfach zu verwenden, und gewähren Sie Benutzern unterschiedliche Zugriffsebenen für das Postfach.

- Persönliche Zugriffstoken (wenn IAM Identity Center aktiviert ist) — Persönliche Zugriffstoken anzeigen und löschen.

> **Note**
>
> Wenn Sie Amazon WorkMail in ein AD Connector Connector-Verzeichnis integrieren, können Sie diese Details nicht aus dem bearbeiten AWS Management Console. Instead, you must edit them using your Active Directory management tools. Limitations apply when your organization is in interoperability mode. Weitere Informationen finden Sie unter Beschränkungen im Interoperabilitätsmodus.

Um die Benutzerdetails zu bearbeiten

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann die Organisation aus, die Sie verwenden möchten.
3. Wählen Sie im Navigationsbereich Benutzer und dann den Namen des Benutzers aus, den Sie bearbeiten möchten.

Um persönliche Daten zu bearbeiten

1. Wählen Sie im Abschnitt Benutzerdetails die Option Bearbeiten aus.
2. Geben Sie unter Benutzerdetails die persönlichen Daten des Benutzers nach Bedarf ein oder ändern Sie sie.
3. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Um eine Verbindung zu einem IAM Identity Center-Benutzer herzustellen

1. Wählen Sie unter Benutzerdetails die Option Bearbeiten aus.

2. Geben Sie die Benutzer-ID des IAM Identity Center-Benutzers ein, den Sie zuordnen möchten. Sie können diese Informationen in der Tabelle Zugewiesene Benutzer auf der IAM Identity Center-Seite oder in der IAM Identity Center-Konsole einsehen.
3. Wählen Sie Änderungen speichern.

Um Postfachkontingente zu bearbeiten

1. Wählen Sie unter Benutzerdetails die Registerkarte Kontingent und dann Bearbeiten aus.
2. Geben Sie im Feld Postfachkontingent aktualisieren eine Größe für das Postfach ein. Sie können Werte von **1** bis eingeben**51200**.
3. Wählen Sie Änderungen speichern.

Um Daten auf Mobilgeräten zu verwalten

> **Note**
>
> Um Mobilgeräte zu verwalten, müssen Ihre Benutzer zunächst ihre Geräte mit Ihrer Amazon-Instance verbinden WorkMail. Informationen zum Verbinden von Mobilgeräten finden Sie unter Mobilgeräteclients für Amazon einrichten WorkMail.

1. Wählen Sie unter Benutzerdetails den Tab Mobilgeräte aus.
2. Um eine aktuelle Geräteliste anzuzeigen, wählen Sie Aktualisieren.
3. Um die Details eines Geräts anzuzeigen, wählen Sie den Gerätenamen aus der Spalte Geräte-ID aus.
4. Um das Gerät zu entfernen oder zu löschen, wählen Sie das Optionsfeld neben dem Gerätenamen und wählen Sie dann je nach Bedarf Entfernen oder Löschen.
5. Bestätigen Sie im daraufhin angezeigten Dialogfeld den Entfernungs- oder Löschvorgang. Denken Sie daran, dass Benutzer wieder angezeigt werden, wenn sie ihre Geräte WorkMail erneut mit Amazon synchronisieren.

So bearbeiten Sie Postfachberechtigungen

1. Wählen Sie die Registerkarte Berechtigungen.
2. Führen Sie eine der folgenden Aktionen aus:

1. Um Berechtigungen hinzuzufügen, wählen Sie Berechtigungen hinzufügen. Öffnen Sie die Liste Neue Berechtigungen hinzufügen und wählen Sie einen Benutzer oder eine Gruppe aus, wählen Sie die Berechtigungseinstellungen für den Benutzer oder die Gruppe aus und klicken Sie dann auf Speichern.
2. Um Benutzerberechtigungen zu bearbeiten, klicken Sie auf die Schaltfläche neben dem Namen des Benutzers. Wählen Sie Bearbeiten, wählen Sie die gewünschten Optionen aus und klicken Sie dann auf Speichern.

   Weitere Informationen zu den Berechtigungsoptionen finden Sie unterArbeiten mit Postfachberechtigungen.
3. Um alle Berechtigungen zu entfernen, wählen Sie Entfernen und bestätigen Sie dann das Entfernen.

Um persönliche Zugriffstoken zu löschen

> **Note**
>
> Stellen Sie sicher, dass das Token, das Sie löschen, von keinem E-Mail-Client aktiv verwendet wird. Wenn Sie ein Token löschen, wenn es verwendet wird, wird die Authentifizierung für die Clients, die das Token verwenden, unterbrochen.

1. Wählen Sie den Tab Personal Access Tokens.
2. Wählen Sie aus der Liste der persönlichen Zugriffstoken das persönliche Zugriffstoken aus, das Sie löschen möchten.
3. Wählen Sie Token löschen.
4. Geben Sie Type in das Bestätigungstextfeld ein.

Das Benutzerkennwort wird zurückgesetzt

Wenn ein Benutzer sein Passwort vergisst oder Probleme hat, sich bei Amazon anzumelden WorkMail, können Sie sein Passwort zurücksetzen.

> **Note**
>
> - Wenn Sie Amazon WorkMail in ein AD Connector Connector-Verzeichnis integriert haben, müssen Sie das Benutzerkennwort in Active Directory zurücksetzen.
> - Wenn Sie Amazon WorkMail mit IAM Identity Center integriert haben, können Sie das Benutzerkennwort zurücksetzen. Weitere Informationen finden Sie unter Zurücksetzen des IAM Identity Center-Benutzerpassworts für einen Endbenutzer im AWS IAM Identity Center Benutzerhandbuch.

To reset a user password

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Klicken Sie im Navigationsbereich auf Users (Benutzer).
4. Aktivieren Sie in der Benutzerliste das Kontrollkästchen neben dem Namen des Benutzers und wählen Sie dann Passwort zurücksetzen aus.
5. Geben Sie im Dialogfeld „Passwort zurücksetzen“ das neue Passwort ein und wählen Sie dann „Zurücksetzen“.

Fehlerbehebung bei WorkMail Amazon-Passwortrichtlinien

If resetting the password is unsuccessful, verify that the new password meets the password policy requirements.

Die Anforderungen an die Passwortrichtlinie hängen davon ab, welchen Verzeichnistyp Ihre WorkMail Amazon-Organisation verwendet.

Passwortrichtlinie für WorkMail Amazon-Verzeichnis und Simple AD AD-Verzeichnis

Standardmäßig müssen Passwörter für ein WorkMail Amazon-Verzeichnis oder Simple AD AD-Verzeichnis wie folgt lauten:

- Nicht leer
- Mindestens acht Zeichen
- Weniger als 64 Zeichen
- Besteht aus lateinischen Grundzeichen oder lateinischen Zusatzzeichen

Passwords must also contain characters from three out of five of the following groups:

- Uppercase characters
- Lowercase characters
- Numerische Ziffern (0 bis 9)
- Special characters (for example, <, ~, or !)
- Latin-1 supplement characters (for example, é, ü, or ñ)

Die Passwortrichtlinien für WorkMail Amazon-Verzeichnisse können nicht geändert werden.

Um eine Simple AD-Passwortrichtlinie zu ändern, verwenden Sie die AD-Verwaltungstools auf einer Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instance Ihres Simple AD AD-Verzeichnisses. Weitere Informationen finden Sie unter Installation der Active Directory-Verwaltungstools im AWS Directory Service Administratorhandbuch.

AWS Managed Microsoft AD Passwortrichtlinie für Verzeichnisse

Informationen zur Standardkennwortrichtlinie für ein AWS Managed Microsoft AD Verzeichnis finden Sie unter Kennwortrichtlinien verwalten für AWS Managed Microsoft AD im AWS Directory Service Administratorhandbuch.

AD Connector-Passwortrichtlinie

AD Connector verwendet die Kennwortrichtlinie der Active Directory-Domäne, mit der er verbunden ist. Weitere Informationen zu den Einstellungen für Kennwortrichtlinien finden Sie in der Dokumentation zu Ihrer Active Directory-Domäne.

Working with notifications

Mit der Amazon WorkMail Push Notifications API können Sie Push-Benachrichtigungen über Änderungen in Ihrem Postfach erhalten, einschließlich neuer E-Mail- und Kalenderaktualisierungen. Sie müssen die URLs (oder die Antworten auf Push-Benachrichtigungen) registrieren, um

Benachrichtigungen zu erhalten. Mit dieser Funktion können Entwickler responsive Anwendungen für WorkMail Amazon-Benutzer erstellen, da Anwendungen schnell über Änderungen aus dem Postfach eines Benutzers informiert werden.

For more information, see Notification subscriptions, mailbox events, and EWS in Exchange.

Sie können bestimmte Ordner abonnieren, z. B. Posteingang oder Kalender, oder alle Ordner für Postfachänderungsereignisse (einschließlich Neue E-Mail, Erstellt und Geändert).

Sie können Clientbibliotheken wie die EWS Java API oder die Managed EWS C# API verwenden, um auf diese Funktion zuzugreifen. Eine vollständige Beispielanwendung eines Push-Responders, entwickelt mit AWS Lambda und API Gateway (unter Verwendung des AWS Serverless Framework), ist auf der Seite verfügbar. AWS GitHub It uses the EWS Java API.

The following is a sample push subscription request:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://
schemas.microsoft.com/exchange/services/2006/types">
   <soap:Body>
      <m:Subscribe xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages">
         <m:PushSubscriptionRequest>
            <t:FolderIds>
               <t:DistinguishedFolderId Id="inbox" />
            </t:FolderIds>
            <t:EventTypes>
               <t:EventType>NewMailEvent</t:EventType>
               <t:EventType>CopiedEvent</t:EventType>
               <t:EventType>CreatedEvent</t:EventType>
               <t:EventType>DeletedEvent</t:EventType>
               <t:EventType>ModifiedEvent</t:EventType>
               <t:EventType>MovedEvent</t:EventType>
            </t:EventTypes>
            <t:StatusFrequency>1</t:StatusFrequency>
            <t:URL>https://YOUR_PUSH_RESPONDER_URL</t:URL>
         </m:PushSubscriptionRequest>
      </m:Subscribe>
   </soap:Body>
</soap:Envelope>
```

The following is a successful subscription request result:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
   <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
      <ServerVersionInfo xmlns="http://schemas.microsoft.com/exchange/
services/2006/types" MajorVersion="14" MinorVersion="2" MajorBuildNumber="390"
 Version="Exchange2010_SP2" MinorBuildNumber="3" />
   </Header>
   <soap:Body>
      <m:SubscribeResponse xmlns:m="http://schemas.microsoft.com/exchange/
services/2006/messages" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types">
         <m:ResponseMessages>
            <m:SubscribeResponseMessage ResponseClass="Success">
               <m:ResponseCode>NoError</m:ResponseCode>
               <m:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</m:SubscriptionId>
               <m:Watermark>AAAAAAA=</m:Watermark>
            </m:SubscribeResponseMessage>
         </m:ResponseMessages>
      </m:SubscribeResponse>
   </soap:Body>
</soap:Envelope>
```

Afterwards, notifications are sent to the URL specified in the subscription request. The following is a sample notification:

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <t:RequestServerVersion
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
 Version="Exchange2010_SP2">
        </t:RequestServerVersion>
    </soap:Header>
    <soap:Body>
        <m:SendNotification
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
            <m:ResponseMessages>
                <m:SendNotificationResponseMessage ResponseClass="Success">
                    <m:ResponseCode>NoError</m:ResponseCode>
```

```
                    <m:Notification>
                        <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</
t:SubscriptionId>
                        <t:PreviousWatermark>ygwAAAAAAAA=</t:PreviousWatermark>
                        <t:MoreEvents>false</t:MoreEvents>
                        <t:ModifiedEvent>
                            <t:Watermark>ywwAAAAAAAA=</t:Watermark>
                            <t:TimeStamp>2018-02-02T15:15:14Z</t:TimeStamp>
                            <t:FolderId Id="AAB2L089bS1kNDgxOGYwOGE5OTQ0="></
t:FolderId>
                            <t:ParentFolderId Id="AAB2L089bS1kNDgxOGYwOGE="></
t:ParentFolderId>
                        </t:ModifiedEvent>
                    </m:Notification>
                </m:SendNotificationResponseMessage>
            </m:ResponseMessages>
        </m:SendNotification>
    </soap:Body>
</soap:Envelope>
```

To acknowledge that the push notification responder has received the notification, it must reply with the following:

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>OK</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

To unsubscribe from receiving push notifications, clients must send an unsubscribe response in the `SubscriptionStatus` field, similar to the following:

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>Unsubscribe</SubscriptionStatus>
      </SendNotificationResult>
```

```
    </s:Body>
  </s:Envelope>
```

Um den Zustand Ihres Push-Benachrichtigungs-Responders zu überprüfen, WorkMail sendet Amazon einen „Heartbeat“ (auch a `StatusEvent` genannt). The frequency with which they are sent is determined by the `StatusFrequency` parameter provided in the initial subscription request. Wenn beispielsweise „`StatusFrequency`gleich“ ist**1**, `StatusEvent` wird alle 1 Minute ein gesendet. This value can range between 1 and 1440 minutes. Das `StatusEvent` sieht wie folgt aus:

```
<?xml version="1.0 (http://www.w3.org/TR/REC-xml/)" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
    <t:RequestServerVersion xmlns:t="http://schemas.microsoft.com/exchange/
services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages" Version="Exchange2010_SP2"/>
</soap:Header>
<soap:Body>
    <m:SendNotification xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
    <m:ResponseMessages>
        <m:SendNotificationResponseMessage ResponseClass="Success">
            <m:ResponseCode>NoError</m:ResponseCode>
            <m:Notification>
                <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</t:SubscriptionId>
                <t:PreviousWatermark>AAAAAAAAAAA=</t:PreviousWatermark>
                <t:MoreEvents>false</t:MoreEvents>
                <t:StatusEvent>
                    <t:Watermark>AAAAAAAAAAA=</t:Watermark>
                </t:StatusEvent>
            </m:Notification>
        </m:SendNotificationResponseMessage>
    </m:ResponseMessages>
</m:SendNotification>
</soap:Body>
</soap:Envelope>
```

Wenn ein Client-Push-Benachrichtigungs-Responder nicht mit demselben 0K Status wie zuvor antwortet, wird die Benachrichtigung für maximal einige Minuten wiederholt. `StatusFrequency` Wenn z. B. `StatusFrequency` gleich 5 ist und die erste Benachrichtigung fehlschlägt, wird sie für maximal 5 Minuten mit einem exponentiellen Backoff zwischen den einzelnen Wiederholungsversuchen wiederholt. Wenn die Benachrichtigung nach Ablauf der Wiederholungszeit

nicht zugestellt wird, ist das Abonnement ungültig und es werden keine neuen Benachrichtigungen zugestellt. You must create a new subscription to continue to receive notifications about mailbox events. Currently, you can subscribe for a maximum of three subscriptions per mailbox.

Enabling signed or encrypted email

Sie können S/MIME verwenden, um es Benutzern zu ermöglichen, signierte oder verschlüsselte E-Mails sowohl innerhalb als auch außerhalb der Organisation zu versenden.

> **Note**
>
> User certificates in the Global Address List (GAL) are supported only in a connected Active Directory setup.

To enable users to send signed or encrypted emails

1. Set up an Active Directory (AD) Connector. Setting up an AD Connector with your on-premises directory allows users to continue to use their existing corporate credentials.
2. Konfigurieren Sie die automatische Registrierung von Zertifikaten so, dass Benutzerzertifikate automatisch im Active Directory ausgestellt und gespeichert werden. Amazon WorkMail erhält Benutzerzertifikate aus dem Active Directory und veröffentlicht sie in der GAL. For more information, see Configure Certificate Autoenrollment.
3. Verteilen Sie die generierten Zertifikate an Benutzer, indem Sie die Zertifikate vom Server, auf dem Microsoft Exchange ausgeführt wird, exportieren und per Post versenden.
4. Each user installs the certificate to their email program (such as Windows Outlook) and mobile devices.

Arbeiten mit -Gruppen

Sie können Gruppen als Verteilerlisten in Amazon verwenden, um E-Mails WorkMail für generische E-Mail-Adressen wie `<sales@example.com>` oder `<support@example.com>` zu empfangen. Sie können mehrere E-Mail-Aliasse für eine Gruppe erstellen.

Darüber hinaus können Sie Gruppen als Sicherheitsgruppen nutzen, um einen Posteingang oder Kalender für ein bestimmtes Team freizugeben.

Gruppen haben keine eigenen Postfächer, und das wirkt sich auf die Postfachberechtigungen aus, die Sie einer Gruppe gewähren können. Informationen zum Einrichten von Postfachberechtigungen für eine Gruppe finden Sie unterVerwaltung von Postfachberechtigungen für Gruppen.

> **Note**
>
> Es kann bis zu zwei Stunden dauern, bis neu hinzugefügte Gruppen in Ihrem Offline-Adressbuch von Microsoft Outlook angezeigt werden.

Themen

- Eine Liste von Gruppen anzeigen
- Eine Gruppe hinzufügen
- Gruppen aktivieren
- Mitglieder zu einer Gruppe hinzufügen
- Gruppendetails bearbeiten
- Mitglieder aus einer Gruppe entfernen
- Gruppenaliase verwalten
- Gruppen deaktivieren
- Löschen einer Gruppe

Eine Liste von Gruppen anzeigen

Um die Liste der Gruppen einzusehen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz.

2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich die Option Groups (Gruppen).
4. Darüber hinaus können Sie Gruppen nach Gruppenname oder primärer E-Mail-Adresse filtern.

> **Note**
>
> Bei der Suche wird Groß- und Kleinschreibung beachtet.

Eine Gruppe hinzufügen

Sie können Gruppen von der WorkMail Amazon-Konsole aus hinzufügen.

So fügen Sie eine Gruppe hinzu

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie bei Bedarf die AWS-Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Gruppen und dann Gruppe hinzufügen aus.

   Die Seite Gruppe hinzufügen wird angezeigt.
4. Geben Sie unter Gruppenname einen Namen für die Gruppe ein.
5. Geben Sie unter E-Mail-Adresse die primäre E-Mail-Adresse für die Gruppe ein.
6. Überprüfen Sie die E-Mail-Adresse der Gruppe und aktualisieren Sie sie bei Bedarf.
7. Standardmäßig wird die Gruppe in der globalen Adressliste angezeigt. Um die Gruppe aus der globalen Adressliste auszublenden, deaktivieren Sie das Kontrollkästchen In globaler Adressliste anzeigen.
8. Wählen Sie Add Group (Gruppe hinzufügen) aus.

Gruppen aktivieren

Wenn Sie Amazon WorkMail in Ihr Unternehmens-Active Directory integrieren oder wenn Sie bereits Gruppen in Ihrem einfachen Active Directory verfügbar haben, können Sie diese Gruppen als Sicherheitsgruppen oder Verteilerlisten in Amazon verwenden WorkMail.

So aktivieren Sie eine vorhandene Verzeichnisgruppe

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich die Option Groups (Gruppen).
4. Aktivieren Sie das Kontrollkästchen neben der Gruppe, die Sie aktivieren möchten, und wählen Sie dann Aktivieren aus.

   Das Dialogfeld „Gruppen aktivieren“ wird angezeigt, in dem Sie aufgefordert werden, den Vorgang zu bestätigen.
5. Überprüfen und ändern Sie bei Bedarf die primäre E-Mail-Adresse für jede Gruppe und wählen Sie dann Aktivieren aus.

Mitglieder zu einer Gruppe hinzufügen

Nachdem Sie eine WorkMail Amazon-Gruppe erstellt und aktiviert haben, verwenden Sie die WorkMail Amazon-Konsole, um Mitglieder zu dieser Gruppe hinzuzufügen.

> **Note**
>
> Wenn Amazon in einen verbundenen Active Directory-Dienst oder Microsoft Active Directory integriert WorkMail ist, können Sie Active Directory zur Verwaltung Ihrer Gruppenmitglieder verwenden. Es kann jedoch länger dauern, bis Änderungen auf Amazon WorkMail übertragen werden.

Um Mitglieder zu einer Gruppe hinzuzufügen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich die Option Groups (Gruppen).
4. Wählen Sie den Namen der Gruppe aus.
5. Wählen Sie auf der Seite mit den Gruppendetails den Tab Mitglieder aus.
6. Wählen Sie unter Gruppe oder Benutzer eine Gruppe oder einen Benutzer aus, den Sie hinzufügen möchten.
7. Wählen Sie den Benutzer oder die Gruppe aus der Drop-down-Liste aus.
8. Wählen Sie Save (Speichern) aus.

Es kann einige Minuten dauern, bis Ihre Änderungen wirksam werden.

Gruppendetails bearbeiten

Sie können die Details einer Gruppe bearbeiten.

Um Gruppendetails zu bearbeiten

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Gruppen und dann die Gruppe aus, die Sie bearbeiten möchten.
4. Aktualisieren Sie auf der Seite mit den Gruppendetails die E-Mail-Adresse nach Bedarf.

5. Standardmäßig werden Gruppen in der globalen Adressliste angezeigt. Um die Gruppe aus der globalen Adressliste auszublenden, deaktivieren Sie das Kontrollkästchen In globaler Adressliste anzeigen.
6. Wählen Sie Änderungen speichern.

Mitglieder aus einer Gruppe entfernen

Verwenden Sie die WorkMail Amazon-Konsole, um Mitglieder aus einer Gruppe zu entfernen.

> **Note**
>
> Wenn Amazon in ein verbundenes Active Directory oder Microsoft Active Directory integriert WorkMail ist, können Sie Active Directory verwenden, um Ihre Gruppenmitglieder zu verwalten. Dadurch kann jedoch die Zeit gespart werden, die benötigt wird, um Ihre Änderungen an Amazon WorkMail weiterzugeben.

Um Mitglieder aus einer Gruppe zu entfernen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Gruppen und dann den Namen der Gruppe aus.
4. Wählen Sie auf der Seite mit den Gruppendetails den Tab Mitglieder aus.
5. Wählen Sie das Mitglied aus, das Sie aus der Gruppe entfernen möchten.
6. Wählen Sie Remove (Entfernen) aus.

Es kann einige Minuten dauern, bis Ihre Änderungen wirksam werden.

Gruppenaliase verwalten

Sie können E-Mail-Aliase zu Gruppen hinzufügen oder entfernen.

Um einer Gruppe einen E-Mail-Alias hinzuzufügen.

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, für die Sie einen Alias hinzufügen möchten.
3. Wählen Sie im Navigationsbereich Gruppen und dann den Namen der Gruppe aus, zu der Sie einen Alias hinzufügen möchten.
4. Wählen Sie im Abschnitt Gruppendetails die Option Aliase aus.
5. Wählen Sie unter Aliase die Option Alias hinzufügen aus.
6. Geben Sie im Feld Alias einen Alias ein.
7. Wählen Sie eine Domain für einen Alias aus.
8. Wählen Sie Hinzufügen aus.

Um E-Mail-Aliase aus einer Gruppe zu entfernen.

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, aus der Sie einen Alias entfernen möchten.
3. Wählen Sie im Navigationsbereich Gruppen und anschließend den Namen der Gruppe aus, aus der Sie Aliase entfernen möchten.
4. Wählen Sie im Abschnitt Gruppendetails die Option Aliase aus.
5. Aktivieren Sie unter Aliase das Kontrollkästchen für die Aliase, die Sie entfernen möchten.
6. Wählen Sie Remove (Entfernen) aus.
7. Überprüfen Sie die Aliase, die entfernt werden sollen.
8. Wählen Sie im Fenster Aliase entfernen die Option Entfernen.

Gruppen deaktivieren

Wenn Sie eine Gruppe nicht mehr benötigen, können Sie sie deaktivieren.

So deaktivieren Sie eine Gruppe

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich die Option Groups (Gruppen).
4. Wählen Sie unter Gruppenname die Gruppen aus, die Sie deaktivieren möchten, und wählen Sie dann Deaktivieren aus.
5. klicken Sie im Dialogfeld Disable group(s) auf Disable.

Löschen einer Gruppe

Bevor Sie eine Gruppe löschen können, müssen Sie diese Gruppe zunächst deaktivieren. Informationen zum Deaktivieren von Gruppen finden Sie unterGruppen deaktivieren.

So löschen Sie eine Gruppe

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich die Option Groups (Gruppen).
4. Aktivieren Sie das Kontrollkästchen neben der deaktivierten Gruppe, die Sie löschen möchten, und wählen Sie Löschen aus.

   Das Dialogfeld Löschen wird angezeigt.
5. Geben Sie im Feld Geben Sie den Gruppennamen ein, um das Löschen zu bestätigen, den Namen der Gruppe ein und wählen Sie dann Löschen aus.

> **Note**
>
> Um eine Gruppe dauerhaft zu löschen, verwenden Sie die `DeleteGroup` API-Aktion für Amazon WorkMail. Weitere Informationen finden Sie DeleteGroupin der Amazon WorkMail API-Referenz.

Arbeiten mit -Ressourcen

Amazon WorkMail kann Ihren Benutzern helfen, Ressourcen zu reservieren. Benutzer können beispielsweise Besprechungsräume oder Geräte wie Projektoren, Telefone oder Autos reservieren. Um eine Ressource zu buchen, fügt der Benutzer die Ressource der Besprechungseinladung hinzu.

Themen

- Eine Liste von Ressourcen anzeigen
- Eine Ressource hinzufügen
- Ressourcendetails bearbeiten
- Ressourcen-Aliase verwalten
- Eine Ressource aktivieren
- Eine Ressource deaktivieren
- Eine Ressource wird gelöscht

Eine Liste von Ressourcen anzeigen

Um die Liste der Ressourcen einzusehen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Resources aus.
4. Darüber hinaus können Sie Ressourcen nach Ressourcenname oder primärer E-Mail-Adresse filtern.

> **Note**
>
> Bei der Suche wird Groß- und Kleinschreibung beachtet.

Eine Ressource hinzufügen

Sie können Ihrer Organisation eine neue Ressource hinzufügen und es Ihren Benutzern ermöglichen, sie zu reservieren.

So fügen Sie eine Ressource hinzu

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Ressourcen und dann Ressource hinzufügen aus.

   Die Seite „Ressource hinzufügen“ wird angezeigt.
4. Geben Sie im Feld Ressourcenname einen Namen für die Ressource ein.
5. Geben Sie optional in das Feld Beschreibung der Ressource eine Beschreibung für die Ressource ein.
6. Wählen Sie unter Ressourcentyp eine Option aus.
7. Überprüfen Sie die E-Mail-Adresse der Ressource und aktualisieren Sie sie bei Bedarf.
8. Standardmäßig wird die Ressource in der globalen Adressliste angezeigt. Um die Ressource aus der globalen Adressliste auszublenden, deaktivieren Sie das Kontrollkästchen In globaler Adressliste anzeigen.
9. Wählen Sie Add resource (Ressource hinzufügen) aus.

Ressourcendetails bearbeiten

Sie können die allgemeinen Details einer Ressource bearbeiten, darunter Name, Beschreibung, Typ und E-Mail-Adresse, Buchungsoptionen und Delegierte.

So bearbeiten Sie allgemeine Ressourcendetails

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.

2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Klicken Sie im Navigationsbereich auf Resources und wählen Sie dann die zu bearbeitende Ressource aus.
4. Aktualisieren Sie auf der Seite mit den Ressourcendetails den Ressourcennamen, die Beschreibung, den Ressourcentyp oder die E-Mail-Adresse nach Bedarf.
5. Standardmäßig werden Ressourcen in der globalen Adressliste angezeigt. Um die Ressource aus der globalen Adressliste auszublenden, deaktivieren Sie das Kontrollkästchen In globaler Adressliste anzeigen.
6. Wählen Sie Änderungen speichern.

Sie können eine Ressource so konfigurieren, dass sie Buchungsanfragen automatisch annimmt oder ablehnt.

Sie können die Buchungsoptionen der Ressource bearbeiten.

Um die Buchungsoptionen einer Ressource zu ändern

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Klicken Sie im Navigationsbereich auf Resources und wählen Sie dann die zu bearbeitende Ressource aus. Eine Seite mit Ressourcendetails wird angezeigt.
4. Wählen Sie unter Buchungsoptionen die Option Bearbeiten aus.
5. Aktivieren oder deaktivieren Sie je nach Bedarf das Kontrollkästchen neben einer Option, um die Option zu aktivieren oder zu deaktivieren.

> **Note**
>
> Wenn Sie eine der automatischen Buchungsoptionen deaktivieren, müssen Sie einen Beauftragten für die Bearbeitung der Buchungsanfragen einrichten. In den nächsten Schritten wird erklärt, wie Sie einen Delegierten erstellen.

Sie können einen Delegierten hinzufügen, um Buchungsanfragen für eine Ressource zu steuern, für die keine automatischen Buchungsoptionen konfiguriert sind. Ressourcendelegierte erhalten automatisch Kopien aller Buchungsanfragen und haben vollen Zugriff auf den Ressourcenkalender. Außerdem müssen sie alle Buchungsanfragen für eine Ressource annehmen.

So fügen Sie einen Ressourcendelegierten hinzu

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Ressourcen und dann den Namen der Ressource aus, zu der Sie einen Delegierten hinzufügen möchten.
4. (Optional) Wählen Sie auf der Registerkarte Buchungsoptionen die Option Bearbeiten aus, deaktivieren Sie das Kontrollkästchen Alle Ressourcenanfragen automatisch annehmen, und wählen Sie dann Speichern aus.
5. Wählen Sie die Registerkarte „Delegierte“ und dann „Delegierten hinzufügen“.

   Das Dialogfeld „Stellvertreter hinzufügen“ wird angezeigt.
6. Öffnen Sie die Liste „Stellvertreter suchen“, wählen Sie einen Delegierten aus und klicken Sie dann auf Speichern.

Um einen Ressourcendelegierten zu entfernen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.

2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, aus der Sie Delegierte entfernen möchten.
3. Wählen Sie im Navigationsbereich Ressourcen und dann den Namen der Ressource aus, aus der Sie einen Delegierten entfernen möchten.
4. Wählen Sie Delegierte und dann den Delegierten aus, den Sie entfernen möchten.
5. Wählen Sie „Entfernen“.

Ressourcen-Aliase verwalten

Sie können E-Mail-Aliase zu Ressourcen hinzufügen oder entfernen.

Um einer Ressource einen E-Mail-Alias hinzuzufügen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, der Sie einen Alias hinzufügen möchten.
3. Wählen Sie im Navigationsbereich Ressourcen und dann den Namen der Ressource aus, der Sie einen Alias hinzufügen möchten.
4. Wählen Sie im Abschnitt Ressourcendetails die Option Aliase aus.
5. Wählen Sie unter Aliase die Option Alias hinzufügen aus.
6. Geben Sie im Feld Alias einen Alias ein.
7. Wählen Sie eine Domain für einen Alias aus.
8. Wählen Sie Hinzufügen aus.

Um E-Mail-Aliase aus einer Ressource zu entfernen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.

2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, aus der Sie Aliase entfernen möchten.
3. Wählen Sie im Navigationsbereich Ressourcen aus, und wählen Sie dann den Namen der Ressource aus, aus der Sie Aliase entfernen möchten.
4. Wählen Sie im Abschnitt Ressourcendetails die Option Aliase aus.
5. Aktivieren Sie unter Aliase das Kontrollkästchen für die Aliase, die Sie entfernen möchten.
6. Wählen Sie Remove (Entfernen) aus.
7. Überprüfen Sie die Aliase, die entfernt werden sollen.
8. Wählen Sie im Fenster Aliase entfernen die Option Entfernen aus.

Eine Ressource aktivieren

Standardmäßig WorkMail erstellt Amazon eine Ressource. Wenn Sie oder eine andere Person eine Ressource deaktivieren, können Sie die Ressource innerhalb von 30 Tagen wieder aktivieren.

Um eine Ressource zu aktivieren

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen zu Regionen finden Sie unter Regionen und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann die Organisation aus, die die Ressource enthält, die Sie aktivieren möchten.
3. Wählen Sie im Navigationsbereich Resources aus.
4. Wählen Sie in der Ressourcenliste die Schaltfläche neben der Ressource aus, die Sie aktivieren möchten, und wählen Sie dann Aktivieren aus.

   Das Dialogfeld „Ressource aktivieren“ wird angezeigt.
5. Wählen Sie Enable (Aktivieren) aus.

Eine Ressource deaktivieren

Wenn Sie eine Ressource deaktivieren, ist sie für Buchungen nicht mehr verfügbar. Sie können beispielsweise einen Konferenzraum deaktivieren, während er umgebaut wird, und den Raum dann wieder aktivieren, sobald er zur Nutzung verfügbar ist.

Um eine Ressource zu deaktivieren

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen zu Regionen finden Sie unter Regionen und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann die Organisation aus, die die Ressource enthält, die Sie deaktivieren möchten.
3. Wählen Sie im Navigationsbereich Resources aus.
4. Wählen Sie in der Liste der Ressourcen die Schaltfläche neben der Ressource aus, die Sie deaktivieren möchten, und wählen Sie dann Deaktivieren aus.

   Das Dialogfeld „Ressource deaktivieren“ wird angezeigt.
5. Wählen Sie Disable (deaktivieren) aus.

Eine Ressource wird gelöscht

Wenn Sie eine Ressource nicht mehr benötigen, können Sie sie löschen. Sie müssen die Ressource jedoch zuerst deaktivieren. Informationen zum Deaktivieren einer Ressource finden Sie in den Schritten im vorherigen Abschnitt.

So entfernen Sie eine Ressource

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen zu Regionen finden Sie unter Regionen und Endpunkte in der Allgemeine Amazon Web Services-Referenz.

2. Wählen Sie im Navigationsbereich Organizations und dann die gewünschte Organisation aus.
3. Wählen Sie im Navigationsbereich Resources aus.
4. Wählen Sie in der Ressourcenliste die Schaltfläche neben der deaktivierten Ressource aus, die Sie entfernen möchten, und wählen Sie dann Löschen aus.

   Das Dialogfeld „Ressource löschen“ wird angezeigt.
5. Geben Sie im Feld Geben Sie den Ressourcennamen ein, um das Löschen zu bestätigen, den Namen der Ressource ein, die Sie löschen möchten, und wählen Sie dann Ressource löschen aus.

Arbeiten mit IAM Identity Center

Sie können die Multi-Faktor-Authentifizierung (MFA) in Amazon aktivieren, WorkMail indem Sie Ihre WorkMail Amazon-Benutzer mit IAM Identity Center verknüpfen. Weitere Informationen finden Sie unter Was ist IAM Identity Center.

In der folgenden Tabelle werden die Schritte zur Bewältigung verschiedener Szenarien beschrieben.

Szenario	Schritte
WorkMail Amazon-Benutzer dem IAM Identity Center zuordnen	1. IAM Identity Center in Amazon aktivieren WorkMail 2. Zuweisen von IAM Identity Center-Benutzern und -Gruppen zu Amazon-Anwendungen WorkMail 3. WorkMail Amazon-Benutzer mit IAM Identity Center-Benutzern verknüpfen
Bestehende WorkMail Amazon-Nutzer	1. Erstellen Sie IAM Identity Center-Benutzer mit demselben Benutzernamen, gruppieren Sie die Benutzer und weisen Sie die Gruppe der WorkMail Amazon-Anwendung zu. 2. Ordnen Sie die WorkMail Amazon-Benutzer den IAM Identity Center-Benutzern zu.
Bestehende IAM Identity Center-Benutzer	1. Erstellen Sie WorkMail Amazon-Benutzer mit demselben Benutzernamen wie die IAM Identity Center-Benutzer. 2. Weisen Sie die IAM Identity Center-Benutzer oder -Gruppen der WorkMail Amazon-An wendung zu. 3. Ordnen Sie die WorkMail Amazon-Benutzer den IAM Identity Center-Benutzern zu.
Ein externes Verzeichnis mit dem IAM Identity Center verbinden	1. Synchronisieren Sie die externen Verzeichn isbenutzer mit der IAM Identity Center-Gr

Szenario	Schritte
	uppe. Weitere Informationen finden Sie in den Tutorials zu den Identitätsquellen von IAM Identity Center 2. Weisen Sie der WorkMail Amazon-An wendung die IAM Identity Center-Gruppe zu. 3. Connect das externe Verzeichnis mit Amazon WorkMail und stellen Sie sicher, dass die Benutzernamen übereinstimmen 4. Ordnen Sie die WorkMail Amazon-Benutzer den IAM Identity Center-Benutzern zu.

Sobald die oben genannten Schritte abgeschlossen sind, können Sie den Status des IAM Identity Center, einen Link zum AWS IAM Identity Center zur Verwaltung von Benutzern und Gruppen, die URL der MFA-fähigen WorkMail Amazon-Webanwendung, den Authentifizierungsmodus, den Status des persönlichen Zugriffstoken und die Zeitleiste unter IAM Identity Center unter Einstellungen in der Amazon-Konsole einsehen. WorkMail Weitere Informationen zur Verwaltung von MFA in der IAM Identity Center-Konsole finden Sie unter Multi-Faktor-Authentifizierung für IAM Identity Center-Benutzer.

> **Note**
>
> Stellen Sie sicher, dass die Konfiguration zwischen Amazon WorkMail und IAM Identity Center gründlich getestet und verifiziert wurde. Benutzer könnten den Zugriff auf ihre Postfächer verlieren, wenn die Konfiguration nicht korrekt und vollständig ist.

Themen

- IAM Identity Center in Amazon aktivieren WorkMail
- Zuweisen von IAM Identity Center-Benutzern und -Gruppen zu Amazon-Anwendungen WorkMail
- WorkMail Amazon-Benutzer mit IAM Identity Center-Benutzern verknüpfen
- Authentifizierungsmodus
- Konfiguration persönlicher Zugriffstoken
- IAM Identity Center wird deaktiviert

IAM Identity Center in Amazon aktivieren WorkMail

Wenn Sie IAM Identity Center aktivieren, fungiert es als Authentifizierungsebene für die WorkMail Amazon-Benutzer. IAM Identity Center-Benutzer werden getrennt vom WorkMail Amazon-Verzeichnis verwaltet. Es wird empfohlen, in IAM Identity Center und Amazon dieselben Benutzernamen zu verwenden. WorkMail

> **Note**
>
> Stellen Sie sicher, dass Amazon WorkMail und IAM Identity Center in derselben Region eingerichtet sind.

Gehen Sie folgendermaßen vor, um IAM Identity Center zu aktivieren.

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Identity Center aus.

   Die Seite mit den IAM Identity Center-Einstellungen wird angezeigt.
3. Wählen Sie Enable (Aktivieren) aus.

   Das Fenster „IAM Identity Center aktivieren“ wird angezeigt.
4. Wählen Sie Enable (Aktivieren) aus.

   Die Seite mit den Identity Center-Einstellungen wird mit dem Identity Center-Status angezeigt.
5. Um IAM Identity Center-Benutzer und -Gruppen zu Ihrer WorkMail Amazon-Organisation hinzuzufügen, folgen Sie dem Link unter Identity Center-Status. Informationen zum Hinzufügen von Benutzern und Gruppen finden Sie unter Identitäten im IAM Identity Center verwalten. .

Zuweisen von IAM Identity Center-Benutzern und -Gruppen zu Amazon-Anwendungen WorkMail

Wenn Sie IAM Identity Center in Amazon aktivieren WorkMail, WorkMail erstellt es in Ihrem Namen eine Anwendung in IAM Identity Center. Standardmäßig müssen IAM Identity Center-Benutzer dieser Anwendung zugewiesen sein oder zu einer Gruppe gehören, die dieser Anwendung zugewiesen ist, um auf ein Postfach in der WorkMail Amazon-Organisation zugreifen zu können. Weitere Informationen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter AWS Verwaltete Anwendungen.

Sie können Amazon WorkMail auf folgende Weise IAM Identity Center-Benutzer und -Gruppen zuweisen:

- Von IAM Identity Center-Benutzern — Sie können IAM Identity Center-Benutzer Amazon zuweisen. WorkMail
- Nach IAM Identity Center-Gruppe — Sie können Amazon IAM Identity Center-Gruppen zuweisen. WorkMail Durch das Hinzufügen einer Gruppe haben alle Benutzer einer Gruppe Zugriff auf Amazon WorkMail.

  Weitere Informationen zum Hinzufügen von Benutzern und Gruppen finden Sie unter Benutzer, Gruppen und Bereitstellung im IAM Identity Center.

> **Note**
>
> Wenn Sie Ihre bestehende Identitätsquelle mit IAM Identity Center verbinden, lesen Sie Folgendes, bevor Sie Ihre Verzeichnisquelle ändern.
>
> - Ihre Authentifizierung wird vom IAM Identity Center verwaltet.
> - Amazon WorkMail behält alle WorkMail Amazon-Benutzer und -Gruppen.
> - IAM Identity Center behält alle IAM Identity Center-Benutzer, -Gruppen und -Zuweisungen bei.
> - Sie müssen WorkMail Amazon-Benutzer und -Gruppen in der WorkMail Amazon-Konsole verwalten.
> - Sie müssen IAM Identity Center-Benutzer und -Gruppen im IAM Identity Center verwalten.
> - Benutzer ohne IAM Identity Center-Zuweisung oder Benutzerzuordnung können nicht auf Amazon WorkMail zugreifen.

- Sie müssen die MFA-Richtlinienkontrollen im IAM Identity Center verwalten.
- Wenn Sie die IAM Identity Center-Quelle in IAM Identity Center zu und von „Active Directory verwalten“ ändern, müssen Sie die vorhandenen IAM Identity Center-Konfigurationen in Amazon deaktivieren WorkMail und neu konfigurieren, um Ihre WorkMail Amazon-Benutzer mit IAM Identity Center zu verknüpfen.

Benutzer und Gruppen, die mit Ihrem IAM Identity Center-Verzeichnis synchronisiert wurden, können Ihrer WorkMail Amazon-Anwendung zugewiesen werden. Weitere Informationen zur Benutzer- und Gruppenverwaltung von IAM Identity Center finden Sie unter Erste Schritte mit allgemeinen Aufgaben in IAM Identity Center. .

Gehen Sie wie folgt vor, um Amazon WorkMail IAM Identity Center-Benutzer und -Gruppen zuzuweisen.

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Identity Center aus.

   Die Seite mit den IAM Identity Center-Einstellungen wird angezeigt.
3. Wählen Sie Benutzer und Gruppen zuweisen aus.

   Sie können neue Benutzer hinzufügen und zuweisen oder bestehende Benutzer und Gruppen zuweisen.

   - Benutzer zuweisen — Sie können dem Amazon WorkMail einzelne IAM Identity Center-Benutzer zuweisen. Sie können entweder einen neuen IAM Identity Center-Benutzer erstellen oder nach einem vorhandenen Benutzer suchen.
   - Gruppen zuweisen — Sie können Amazon WorkMail auch eine IAM Identity Center-Gruppe zuweisen. Alle Mitglieder der Gruppe werden dann Amazon zugewiesen WorkMail.

> **Note**
>
> Alle neuen IAM Identity Center-Benutzer sind standardmäßig in IAM Identity Center aktiviert. Um Amazon Zugriff zu gewähren WorkMail, müssen Sie ihr Passwort im IAM Identity Center festlegen und sie Amazon WorkMail zuweisen. Weitere Informationen finden Sie unter Benutzer zu Ihrem Identity Center-Verzeichnis hinzufügen.

WorkMail Amazon-Benutzer mit IAM Identity Center-Benutzern verknüpfen

Wenn sich ein Benutzer mit seinen IAM Identity Center-Benutzeranmeldedaten beim Amazon WorkMail Web Client anmeldet, öffnet der Client das Postfach des zugehörigen WorkMail Amazon-Benutzers. Wenn dem IAM Identity Center-Benutzer kein Benutzer in der WorkMail Organisation zugeordnet ist, WorkMail wird eine Verknüpfung zwischen dem sich anmeldenden IAM Identity Center-Benutzer und dem WorkMail Benutzer mit demselben Benutzernamen erstellt, sofern ein WorkMail solcher Benutzer existiert. Andernfalls zeigt der Client dem Benutzer eine Fehlermeldung an.

> **Note**
>
> Es wird empfohlen, denselben Benutzernamen für einen Benutzer in Amazon WorkMail und IAM Identity Center zu verwenden, da die Verknüpfung automatisch erstellt WorkMail wird, wenn sich der Benutzer zum ersten Mal mit seinen IAM Identity Center-Benutzeranmeldedaten am Amazon WorkMail Web Client anmeldet. Wenn die Benutzernamen unterschiedlich sind, sind Sie dafür verantwortlich, die Zuordnung zu erstellen.

Gehen Sie wie folgt vor, um Benutzer zuzuordnen.

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region AWS. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Region und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Identity Center aus.

Die Seite mit den IAM Identity Center-Einstellungen wird angezeigt.

3. Wählen Sie Benutzer zuordnen aus.
4. Wählen Sie unter WorkMail Benutzer auswählen den WorkMail Amazon-Benutzer aus, den Sie verknüpfen möchten.
5. Geben Sie unter Geben Sie die IAM Identity Center-Benutzer-ID ein die ID des IAM Identity Center-Benutzers ein, den Sie zuordnen möchten. Sie können die ID aus dem Tab Zugewiesene Benutzer auf der Identity Center-Seite kopieren.

   > **Note**
   >
   > Der IAM Identity Center-Benutzer muss für den Zugriff auf die WorkMail Amazon-Anwendung autorisiert sein.

6. Wählen Sie Associate users aus.

   Sobald die Verknüpfung erfolgreich ist, kann sich der WorkMail Amazon-Benutzer WorkMail mit den MFA IAM Identity Center-Anmeldeinformationen Amazon Amazon anmelden.

> **Note**
>
> Sie können WorkMail Amazon-Benutzer auch IAM Identity Center-Benutzern zuordnen, wenn Sie die WorkMail Amazon-Benutzerdetails bearbeiten. Weitere Informationen finden Sie unter Editing user details.

Authentifizierungsmodus

Sie können den Authentifizierungsmodus verwenden, um es Benutzern zu ermöglichen, sich entweder mit ihren WorkMail Amazon-Verzeichnisanmeldedaten oder ihren IAM Identity Center-Anmeldeinformationen anzumelden oder die Anmeldung auf nur IAM Identity Center-Anmeldeinformationen zu beschränken.

Bei Amazon sind zwei Authentifizierungsmodi verfügbar WorkMail.

> **Note**
>
> Die Wahl des Authentifizierungsmodus hängt von den Sicherheitsanforderungen und der Benutzererfahrung Ihres Unternehmens ab. Es wird empfohlen, den Modus „Nur IAM Identity Center“ zu verwenden, da er durch die Durchsetzung von IAM Identity Center-Anmeldeinformationen und MFA mehr Sicherheit bietet. Bevor Sie jedoch vom Amazon WorkMail Directory- und IAM Identity Center-Modus wechseln, sollten Sie den MFA-Prozess mit all Ihren Benutzern testen, um einen reibungslosen Übergang zu gewährleisten und jegliche Auswirkungen auf den bestehenden E-Mail-Client-Zugriff zu vermeiden.

- Amazon WorkMail Directory und IAM Identity Center (zum Testen empfohlen) — Dies ist die Standardoption, mit der Sie die IAM Identity Center-Verknüpfungen testen können, bevor Sie in den Produktionsmodus wechseln. Im Testmodus können sich Benutzer sowohl mit dem WorkMail Amazon-Verzeichnis als auch mit den Anmeldeinformationen für das IAM Identity Center beim Amazon WorkMail Web Client anmelden. Wenn Sie die URL der WorkMail Amazon-Webanwendung in den Organisationseinstellungen teilen, kann sich Ihr Benutzer mit seinen WorkMail Amazon-Verzeichnisanmeldedaten anmelden. Wenn Sie die MFA-fähige URL in den IAM Identity Center-Einstellungen teilen, kann sich Ihr Benutzer mit seinen IAM-Anmeldeinformationen anmelden.
- Nur IAM Identity Center (für die Produktion empfohlen) — In diesem Authentifizierungsmodus können Sie sich nur mit den IAM Identity Center-Anmeldeinformationen in das WorkMail Amazon-Kundenpostfach einloggen. Für alle bestehenden WorkMail Amazon-Benutzer sind die Anmeldeinformationen für das WorkMail Amazon-Verzeichnis nicht mehr sowohl für die WorkMail Amazon-Webanwendung als auch für alle vorhandenen E-Mail-Clients gültig. Sie können ein persönliches Zugriffstoken anfordern, um mit beliebigen E-Mail-Clients auf das Postfach zuzugreifen. Um zu verhindern, dass der Zugriff auf Postfächer verloren geht, stellen Sie sicher, dass MFA für alle WorkMail Amazon-Benutzer aktiviert ist.

Gehen Sie folgendermaßen vor, um den Authentifizierungsmodus zu aktivieren.

1. Wählen Sie auf der Seite Identity Center-Einstellungen die Registerkarte Authentifizierungsmodus aus.
2. Wählen Sie Bearbeiten aus.

   Die Seite Authentifizierungsmodus bearbeiten wird angezeigt.

3. Wählen Sie eine der folgenden Optionen:
   - Nur IAM Identity Center
   - Amazon WorkMail Directory und IAM Identity Center
4. Wählen Sie Save aus.

Konfiguration persönlicher Zugriffstoken

Sie können ein persönliches Zugriffstoken aktivieren, damit WorkMail Amazon-Benutzer über Desktop- und mobile E-Mail-Clients auf ihre Postfächer zugreifen können. Nach der Aktivierung von IAM Identity Center wird der Status des persönlichen Zugriffstokens standardmäßig auf aktiv gesetzt und ist 365 Tage gültig. Nach der Aktivierung von IAM Identity Center sind die vorhandenen Anmeldeinformationen Ihrer Benutzer nicht mehr gültig, um sich bei ihren E-Mail-Clients anzumelden. Ihre Benutzer können das persönliche Zugriffstoken aus der WorkMail Amazon-Webanwendung generieren und es verwenden, um sich bei beliebigen E-Mail-Clients anzumelden. Sie können den Ablauf des persönlichen Zugriffstokens bearbeiten, und wenn das Token abläuft, kann Ihr Benutzer ein neues generieren.

> **Note**
>
> - Ihr Benutzer kann Ihr persönliches Zugriffstoken nur einmal ansehen und kopieren, wenn Sie es in Amazon erstellen WorkMail. Wenn Sie Ihr persönliches Zugriffstoken verlieren, müssen Sie aus Sicherheitsgründen ein neues generieren.
> - Amazon erlaubt persönliche Zugriffstoken für den Postfachzugriff WorkMail nur, wenn der WorkMail Amazon-Benutzer einem IAM Identity Center-Benutzer zugeordnet ist, der für den Zugriff auf die WorkMail Amazon-Anwendung autorisiert ist.

Die Konfigurationen der persönlichen Zugriffstoken sind unten aufgeführt:

- Aktiv — Wenn der Status des persönlichen Zugriffstokens auf Aktiv gesetzt ist, kann Ihr Benutzer ein persönliches Zugriffstoken von Amazon generieren WorkMail und es verwenden, um sich innerhalb der Gültigkeitsdauer des Tokens bei einem beliebigen E-Mail-Client anzumelden.
- Inaktiv — Wenn der Status des persönlichen Zugriffstokens auf Inaktiv gesetzt ist, kann Ihr Benutzer keine persönlichen Zugriffstoken für den Zugriff auf Postfächer generieren oder verwenden.

- Gültigkeitsdauer des Tokens — Standardmäßig ist das persönliche Zugriffstoken 365 Tage gültig. Sie haben die Möglichkeit, die Lebensdauer des persönlichen Zugriffstokens zu ändern. Wenn Sie die Einstellung für die Gültigkeitsdauer leer lassen, hat das Token eine unbestimmte Lebensdauer und läuft nie ab.

Gehen Sie wie folgt vor, um persönliche Zugriffstoken zu konfigurieren.

1. Wählen Sie auf der Seite Identity Center-Einstellungen die Registerkarte Konfiguration persönlicher Zugriffstoken aus.
2. Wählen Sie Bearbeiten aus.

   Die Seite Konfiguration des persönlichen Tokens bearbeiten wird angezeigt.
3. Schieben Sie unter Token-Status auf die Schaltfläche Aktiv, um das persönliche Zugriffstoken zu aktivieren.
4. Geben Sie im Textfeld Gültigkeitsdauer des Tokens (in Tagen) die Anzahl der Tage ein, an denen das persönliche Zugriffstoken aktiviert werden kann.
5. Wählen Sie Save aus.

IAM Identity Center wird deaktiviert

Sie können IAM Identity Center von der WorkMail Amazon-Konsole aus deaktivieren. Nach der Deaktivierung können Sie nicht mit den IAM Identity Center-Anmeldeinformationen oder persönlichen Zugriffstoken auf das Postfach zugreifen. Es wird empfohlen, alle Benutzerkennwörter zurückzusetzen, damit die WorkMail Amazon-Benutzer wieder die Anmeldeinformationen für das WorkMail Amazon-Verzeichnis verwenden.

> **Note**
>
> Überprüfen Sie, ob Folgendes der Fall ist:
>
> - Nach der Deaktivierung von IAM Identity Center bleiben Ihre Amazon WorkMail - und IAM Identity Center-Benutzer und -Gruppen unverändert.
> - Die bestehenden Benutzerzuordnungen werden weiterhin bestehen.
> - Ihre Authentifizierung wird wieder vom WorkMail Amazon-Verzeichnis statt vom IAM Identity Center verwaltet.

Gehen Sie folgendermaßen vor, um IAM Identity Center zu deaktivieren.

1. Wählen Sie auf der Seite Identity Center-Einstellungen die Option Deaktivieren aus.

   Die Seite „IAM Identity Center deaktivieren“ wird angezeigt.
2. Wählen Sie Bestätigen aus.

Arbeiten mit mobilen Geräten

In den Themen in diesem Abschnitt wird erklärt, wie Sie mit Amazon verbundene Mobilgeräte verwalten WorkMail.

Themen

- Bearbeiten der Mobilgeräte-Richtlinie Ihrer Organisation
- Managing mobile devices
- Zugriffsregeln für mobile Geräte verwalten
- Überschreibungen für den Zugriff auf mobile Geräte verwalten
- Integration mit Verwaltungslösungen für mobile Geräte

Bearbeiten der Mobilgeräte-Richtlinie Ihrer Organisation

Sie können die Mobilgeräterichtlinie Ihrer Organisation bearbeiten, um die Art und Weise zu ändern, wie Mobilgeräte mit Amazon interagieren WorkMail.

So bearbeiten Sie die Richtlinie für Mobilgeräte in Ihrem Unternehmen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die AWS-Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Regionsname und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich die Option Mobile Policies und dann auf dem Bildschirm Mobile Policy die Option Bearbeiten aus.
4. Aktualisieren Sie die folgenden Elemente, falls erforderlich:

   a. Require encryption on device (Verschlüsseln auf Gerät erforderlich): Verschlüsseln von E-Mail-Daten auf dem Mobilgerät.
   b. Require encryption on storage card (Verschlüsseln auf Speicherkarte erforderlich): Verschlüsseln von E-Mail-Daten auf dem Wechseldatenträger des Mobilgeräts.
   c. Passwort erforderlich: Zum Entsperren eines Mobilgeräts ist ein Passwort erforderlich.
   d. Einfaches Passwort zulassen: Verwenden Sie die PIN des Geräts als Passwort.

e. Minimale Passwortlänge: Legen Sie die Anzahl der Zeichen fest, die für ein gültiges Passwort erforderlich sind.

f. Alphanumerisches Passwort erforderlich: Passwörter, die aus Buchstaben und Zahlen bestehen, sind erforderlich.

g. Anzahl der zulässigen Fehlversuche: Geben Sie die Anzahl der fehlgeschlagenen Versuche zum Entsperren von Geräten an, die zulässig sind, bevor das Gerät des Benutzers gelöscht wird. Alle Daten, einschließlich persönlicher Dateien, werden gelöscht, wenn das Gerät gelöscht wird.

h. Password expiration (Passwortablauf): Geben Sie die Anzahl der Tage an, bevor ein Passwort abläuft und geändert werden muss.

i. Enable screen lock (Bildschirmsperre aktivieren): Geben Sie die Anzahl der Sekunden an, die ohne Benutzereingaben vergehen müssen, um den Bildschirm des Benutzers zu sperren.

j. Enforce password history (Passwortverlauf erzwingen): Geben Sie die Anzahl der Passwörter an, die verwendet werden müssen, bevor dasselbe Passwort wiederholt werden kann.

5. Wählen Sie Save (Speichern) aus.

Managing mobile devices

In den Themen in diesem Abschnitt wird erklärt, wie Sie mobile Geräte per Fernzugriff löschen, Geräte aus Ihrer Organisation entfernen und die Details zu Geräten einsehen können. For information about editing your organization's mobile device policy, see Bearbeiten der Mobilgeräte-Richtlinie Ihrer Organisation.

Themen

- Remotely wiping mobile devices
- Removing user devices from the devices list
- Viewing mobile device details

Remotely wiping mobile devices

In den Schritten in diesem Abschnitt wird erklärt, wie Sie mobile Geräte per Fernzugriff löschen können. Beachten Sie Folgendes:

- Die Geräte müssen online und mit Amazon verbunden sein WorkMail. Wenn jemand die Verbindung zum Gerät trennt, wird der Löschvorgang wieder aufgenommen, wenn der Benutzer das Gerät wieder anschließt.
- Die Übertragung von Löschvorgängen kann fünf Minuten dauern.

> **Important**
>
> For most mobile devices, a remote wipe resets the device to factory defaults. All data, including personal files, can be removed when you perform this procedure.

To remotely wipe a user's mobile device

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die AWS-Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen finden Sie unter Regionsname und Endpunkte in der Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Benutzer aus und wählen Sie in der Benutzerliste den Namen des Benutzers aus, dessen Gerät Sie löschen möchten.
4. Wählen Sie die Registerkarte Mobilgeräte aus.
5. Wählen Sie in der Geräteliste die Schaltfläche neben dem Gerät aus und wählen Sie dann Löschen aus.
6. Prüfen Sie anhand des Status in der Übersicht, ob das Löschen angefordert wurde.
7. Nachdem das Gerät gelöscht wurde, entfernen Sie es aus der Geräteliste. In den Schritten im nächsten Abschnitt wird erklärt, wie das geht.

   > **Important**
   >
   > Wenn Sie ein gelöschtes Gerät wieder in die Geräteliste eines Benutzers aufnehmen möchten, müssen Sie es zunächst aus der Geräteliste entfernen. Andernfalls löscht das System das Gerät erneut.

Removing user devices from the devices list

Wenn jemand ein bestimmtes Mobilgerät nicht mehr verwendet oder Sie das Gerät aus der Ferne gelöscht haben, können Sie das Gerät aus der Geräteliste entfernen. When the user configures the device again, it shows up in the list.

To remove a user's mobile devices from the devices list

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die AWS-Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Benutzer und dann den Namen des Benutzers aus.
4. Wählen Sie die Registerkarte Mobilgeräte aus.
5. Wählen Sie in der Geräteliste die Schaltfläche neben dem Gerät aus und wählen Sie Entfernen.

Viewing mobile device details

Sie können die Details des Mobilgeräts eines Benutzers einsehen.

> **Note**
>
> Manche Geräte senden nicht alle Daten an den Server. Möglicherweise werden nicht alle verfügbaren Gerätedetails angezeigt.

To view device details

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region. Wählen Sie auf der Navigationsleiste die Region aus, die Ihren Anforderungen entspricht. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich Benutzer und dann die Registerkarte Mobilgeräte aus.

4. Wählen Sie in der Geräteliste die ID des Geräts aus, für das Sie Details anzeigen möchten.

   In der folgenden Tabelle sind die Gerätestatuscodes aufgeführt.

Status	Description
PROVISIONING_REQUIRED	Ein Benutzer oder Administrator hat beantragt, dass das Gerät für die Verwendung mit Amazon WorkMail bereitgestellt wird. Geräte werden auch auf diesen Status gesetzt, wenn die aktuelle Richtlinie für dieses Gerät in der WorkMail Amazon-Konsole geändert wird.
PROVISIONING_SUCCEEDED	Das Gerät wurde erfolgreich bereitgestellt. Das Gerät hat die angegebene Richtlinie durchgesetzt.
WIPE_REQUIRED	Ein Administrator hat in der WorkMail Amazon-Konsole eine Löschung angefordert.
WIPE_SUCCEEDED	The device has been successfully wiped.

Zugriffsregeln für mobile Geräte verwalten

Die Zugriffsregeln für mobile Geräte für Amazon WorkMail ermöglichen es Administratoren, den Postfachzugriff für bestimmte Arten von Mobilgeräten zu kontrollieren. Standardmäßig verwendet jede WorkMail Amazon-Organisation eine Regel, die Postfachzugriff auf alle Geräte gewährt, unabhängig von Typ, Modell, Betriebssystem oder Benutzeragent. Sie können diese Standardregel bearbeiten oder durch eine eigene ersetzen. Sie können auch Regeln hinzufügen, ändern und löschen.

> **Warning**
>
> Wenn Sie alle Regeln für den Zugriff auf mobile Geräte für eine Organisation löschen, WorkMail blockiert Amazon den gesamten Zugriff auf mobile Geräte.

Sie können auf der Grundlage der folgenden Geräteeigenschaften Regeln erstellen, die den Zugriff zulassen oder verweigern:

- Gerätetyp — „iPhone“, „iPad“ oder „Android“.
- Gerätemodell — „iPhone 10c1", „iPad 5C1" oder" X“. HTCOne
- Gerätebetriebssystem — „iOS 12.3.1 16F203" oder „Android 8.1.0“.
- Geräte-Benutzeragent — „iOS/14.2 (18B92) exchangesyncd/1.0“ oder „Android-mail/7.7.16.163886392.release“.

Informationen zum Anzeigen der Geräteeigenschaften in der AWS Management Console finden Sie unter Details zu Mobilgeräten anzeigen.

> **Note**
>
> Einige Geräte und Clients melden möglicherweise nicht Eigenschaften für alle Felder. Informationen zur Umgehung dieser Fälle finden Sie unter Dealing with empty fields

> **Important**
>
> Die Amazon-Zugriffsregeln für WorkMail Mobilgeräte gelten nur für Geräte, die das Microsoft ActiveSync Exchange-Protokoll verwenden. Mobile Clients, die ein anderes Protokoll wie IMAP verwenden, melden die hier aufgeführten Geräteeigenschaften nicht, sodass diese Regeln nicht gelten.
> Wenn Sie den Zugriff für Geräte einschränken müssen, die andere Protokolle verwenden, können Sie Zugriffskontrollregeln erstellen. Weitere Informationen zu ihnen finden Sie unter Arbeiten mit Zugriffskontrollregeln. Sie können beispielsweise den Zugriff auf andere Protokolle und Webmail auf einen bestimmten Bereich von Unternehmens-IP-Adressen beschränken, Microsoft aber von einem anderen Ort ActiveSync aus zulassen und dann mithilfe der Zugriffsregeln für mobile Geräte die Typen und Versionen der erlaubten Clients weiter einschränken.

Themen

- So funktionieren die Zugriffsregeln für mobile Geräte
- Verwenden von Zugriffsregeln für mobile Geräte

So funktionieren die Zugriffsregeln für mobile Geräte

Zugriffsregeln für mobile Geräte gelten nur für Geräte, die das Microsoft ActiveSync Exchange-Protokoll verwenden. Jede Regel hat eine Reihe von Bedingungen, die angeben, wann die Regel gilt, sowie einen Zugriffseffekt für das Gerät `ALLOW` oder `DENY` für das Gerät. Eine Regel gilt nur dann für eine Zugriffsanfrage, wenn alle Bedingungen der Regel den Eigenschaften des Mobilgeräts des Benutzers entsprechen. Regeln ohne Bedingungen gelten für alle Anfragen. Jede Bedingung verwendet einen Präfixabgleich ohne Berücksichtigung der Groß- und Kleinschreibung mit den gemeldeten Eigenschaften des Geräts.

Amazon WorkMail bewertet Regeln wie folgt:

- Wenn eine `DENY` Regel mit einer Geräteeigenschaft übereinstimmt, blockiert die Richtlinie das Gerät. `DENY`Regeln haben Vorrang vor `ALLOW` Regeln.
- Wenn mindestens eine `ALLOW` Regel zutrifft und keine `DENY` Regel zutrifft, lässt die Richtlinie das Gerät zu.
- Wenn keine Regel zutrifft, ist das Gerät gesperrt.

> **Important**
>
> Mobilgeräte melden die Eigenschaften, anhand derer die Regeln funktionieren. Die Geräte melden ihre Eigenschaften während des ActiveSync Microsoft-Gerätebereitstellungsprozesses. Amazon WorkMail kann nicht unabhängig überprüfen, ob mobile Clients korrekte up-to-date Informationen melden.

Verwenden von Zugriffsregeln für mobile Geräte

Sie können die AWS-Befehlszeilenschnittstelle (CLI) verwenden APIs , um Zugriffsregeln für mobile Geräte zu erstellen und zu verwalten. Weitere Informationen zu finden Sie im AWS CLIAWS-Benutzerhandbuch für die Befehlszeilenschnittstelle.

> **Important**
>
> Wenn Sie eine Zugriffsregel für eine WorkMail Amazon-Organisation ändern, kann es fünf Minuten dauern, bis die betroffenen Geräte der aktualisierten Regel folgen, und Geräte zeigen während dieser Zeit möglicherweise ein inkonsistentes Verhalten. Sie sehen jedoch

sofort das richtige Verhalten, wenn Sie Regeln testen. Weitere Informationen finden Sie unter Testing mobile device access rules.

Zugriffsregeln für mobile Geräte auflisten

Das folgende Beispiel zeigt, wie die Zugriffsregeln für mobile Geräte aufgelistet werden.

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Zugriffsregeln für mobile Geräte erstellen

Im folgenden Beispiel wird eine Regel erstellt, die verhindert, dass alle Android-Geräte auf Postfächer zugreifen.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

Im folgenden Beispiel wird eine Regel erstellt, die nur eine bestimmte Version von iOS zulässt. Achten Sie darauf, die `ALLOW-all` Standardregel zu entfernen.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

Die Zugriffsregeln für mobile Geräte werden aktualisiert

Im folgenden Beispiel wird eine Geräteregel aktualisiert, indem eine Kennung hinzugefügt wird.

```
aws workmail update-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d --
name AllowLatestiOS --effect ALLOW --device-operating-systems "iOS 14.4"
```

Löschen einer Zugriffsregel für mobile Geräte

Im folgenden Beispiel wird die Zugriffsregel für mobile Geräte mit der angegebenen ID gelöscht.

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

Zugriffsregeln für mobile Geräte werden getestet

Um Zugriffsregeln zu testen, können Sie die GetMobileDeviceAccessEffectAPI oder den Befehl get-mobile-device-access -effect in der AWS CLI verwenden. Weitere Informationen zu finden Sie im AWS CLIBenutzerhandbuch für die AWS Befehlszeilenschnittstelle.

Beim Testen übergeben Sie die Eigenschaften eines simulierten Mobilgeräts, und die API oder CLI gibt den Zugriffseffekt — `ALLOW` oder `DENY` — zurück, den ein echtes Mobilgerät mit diesen Eigenschaften erhalten würde. Mit diesem Befehl wird beispielsweise getestet, ob ein iPhone mit iOS 14.2 und der Standard-E-Mail-App auf ein Postfach zugreifen kann.

```
aws workmail get-mobile-device-access-effect --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --device-type "iPhone" --device-model "iPhone10C1"
 --device-operating-system "iOS 14.2.1 16F203" --device-user-agent "iOS/14.2 (18B92)
 exchangesyncd/1.0"
```

Umgang mit leeren Feldern

Manche Mobilgeräte oder Clients melden möglicherweise keine Informationen für ein oder mehrere Felder, sodass die Werte leer bleiben. Regeln können mit diesen Geräten abgeglichen werden, indem der spezielle Wert `$NONE` in einer Bedingung verwendet wird. Eine Regel mit `DeviceTypes=["iphone", "ipad", "$NONE"]` sucht beispielsweise nach Geräten, die einen Gerätetyp von `"iphone"` oder `"ipad"` oder gar keinen Gerätetyp melden.

Negative Bedingungen wie `NotDeviceTypes` oder stimmen `NotDeviceUserAgents` nicht mit diesen leeren Werten überein. Eine Regel mit `NotDeviceTypes=["android"]` entspricht beispielsweise Geräten, die einen anderen Gerätetyp als melden`"android"`. Die Regel gilt jedoch nicht für Geräte, die überhaupt keinen Gerätetyp melden.

Überschreibungen für den Zugriff auf mobile Geräte verwalten

Sie verwenden Überschreibungen für den Zugriff auf mobile Geräte, um die Ergebnisse der Zugriffsregeln für mobile Geräte außer Kraft zu setzen. Die Überschreibungen gelten für bestimmte Benutzer und Geräte und machen die Standardzugriffsregel rückgängig. Sie können Überschreibungen auch verwenden, um einmalige Ausnahmen für Zugriffsregeln zu erstellen und bestimmte Benutzer- und Gerätepaare zuzulassen oder zu verweigern. Darüber hinaus können

Sie Überschreibungen mit einer Zugriffsregel für `DefaultDenyAll` mobile Geräte verwenden. Dadurch werden Zugriffsentscheidungen auf eine MDM-Lösung (Mobile Device Management) eines Drittanbieters verschoben. Weitere Informationen finden Sie unter Überschreibungen verwalten und Integration mit Verwaltungslösungen für mobile Geräte

Themen

- So funktionieren Überschreibungen für den Zugriff auf mobile Geräte
- Überschreibungen verwalten

So funktionieren Überschreibungen für den Zugriff auf mobile Geräte

Sie erstellen Überschreibungen für den Zugriff auf mobile Geräte für ein bestimmtes Benutzer- und Gerätepaar. Durch die Überschreibung wird das Standardzugriffsergebnis rückgängig gemacht, wenn die Zugriffsregeln für mobile Geräte für einen bestimmten Benutzer und ein bestimmtes Gerät ausgewertet werden. Wenn eine Zugriffsregel beispielsweise normalerweise den Zugriff verweigert, ermöglicht eine Zugriffsüberschreibung dem Benutzer und dem Gerät, ihre E-Mails zu synchronisieren. Umgekehrt können Sie, wenn eine Zugriffsregel normalerweise den Zugriff zulässt, eine Außerkraftsetzung einrichten, die verhindert, dass Benutzer und Gerät ihre E-Mails synchronisieren. Wenn Sie eine Überschreibung des Zugriffs auf Mobilgeräte löschen, respektiert Amazon bei der Entscheidung, ob diesem Benutzer und diesem Gerät Zugriff gewährt werden soll, WorkMail erneut das Ergebnis der aktuellen Regeln für den Zugriff auf mobile Geräte.

> **Important**
>
> Wenn Sie eine Zugriffsüberschreibung für Mobilgeräte für eine WorkMail Amazon-Organisation ändern, kann es fünf Minuten dauern, bis die betroffenen Geräte der aktualisierten Überschreibung folgen.

Überschreibungen verwalten

Überschreibungen für den Zugriff auf mobile Geräte können mithilfe der API oder erstellt, aktualisiert oder gelöscht werden. AWS Command Line Interface Weitere Informationen zu finden Sie im AWS CLIAWS-Benutzerhandbuch für die Befehlszeilenschnittstelle.

Um die Geräte-ID zu finden, verwenden Sie die AWS Management Console. Weitere Informationen finden Sie unter Details zu Mobilgeräten anzeigen.

Auflisten der Überschreibungen für den Zugriff auf mobile Geräte

Dieses Beispiel zeigt, wie alle Zugriffsüberschreibungen für mobile Geräte für eine bestimmte WorkMail Amazon-Organisation aufgelistet werden.

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Überschreibungen für den Zugriff auf mobile Geräte erstellen und aktualisieren

Dadurch wird der Zugriff auf Mobilgeräte außer Kraft gesetzt, sodass der Zugriff auf die angegebene WorkMail Amazon-Organisations-, Benutzer- und Geräte-ID verweigert wird.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect DENY
```

Eine bestehende Überschreibung des Zugriffs auf mobile Geräte kann geändert werden, um einen anderen Effekt zu erzielen. Dadurch wird die zuvor erstellte Zugriffsüberschreibung für mobile Geräte aktualisiert, sodass der Zugriff nicht verweigert wird, sondern ermöglicht.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect ALLOW
```

Löschen von Zugriffsüberschreibungen für mobile Geräte

Dadurch wird die Überschreibung des Zugriffs auf mobile Geräte für die angegebene WorkMail Amazon-Organisation, den angegebenen Benutzer und die angegebene Geräte-ID gelöscht.

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0
```

Integration mit Verwaltungslösungen für mobile Geräte

Amazon WorkMail unterstützt einige grundlegende Funktionen zur Verwaltung mobiler Geräte durch Richtlinien für mobile Geräte und Zugriffsregeln für mobile Geräte. Diese Funktionen können

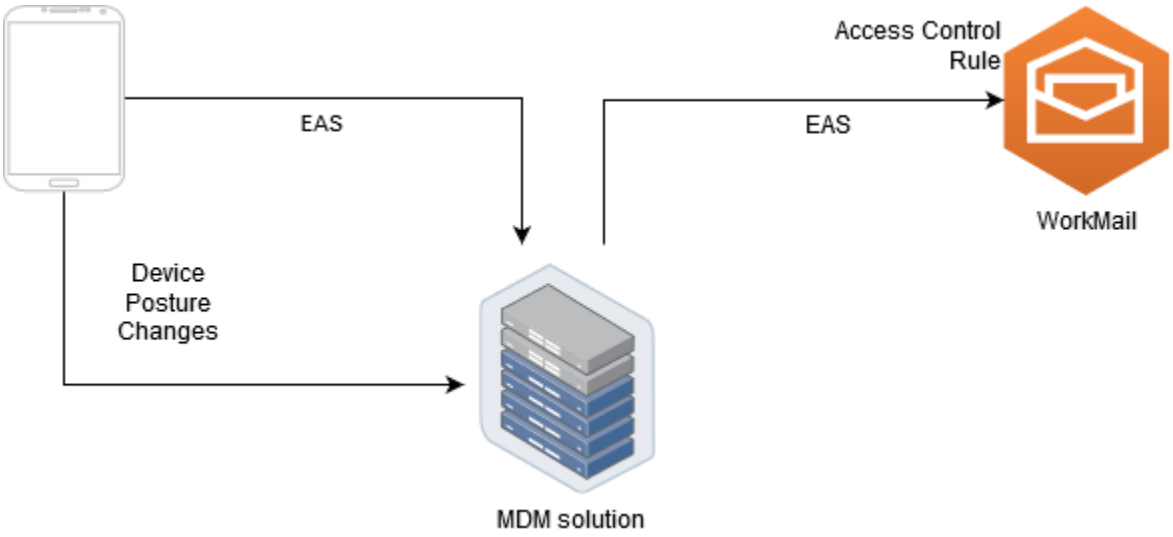
jedoch nur über das Microsoft Exchange ActiveSync (EAS) -Protokoll mit Mobilgeräten interagieren, sodass sie nur begrenzt in der Lage sind, den Sicherheitsstatus der Geräte zu überprüfen und durchzusetzen. Administratoren, die mehr Kontrolle über Gerätesicherheit und Compliance benötigen, können eine MDM-Lösung (Mobile Device Management) eines Drittanbieters verwenden.

Überblick über die Verwaltungslösungen für mobile Geräte

Sie können Ihre MDM-Lösung in zwei Modi konfigurieren: Proxy oder Direct. Schlagen Sie in Ihrer MDM-Dokumentation nach, welche Modi Ihre Lösung unterstützt.

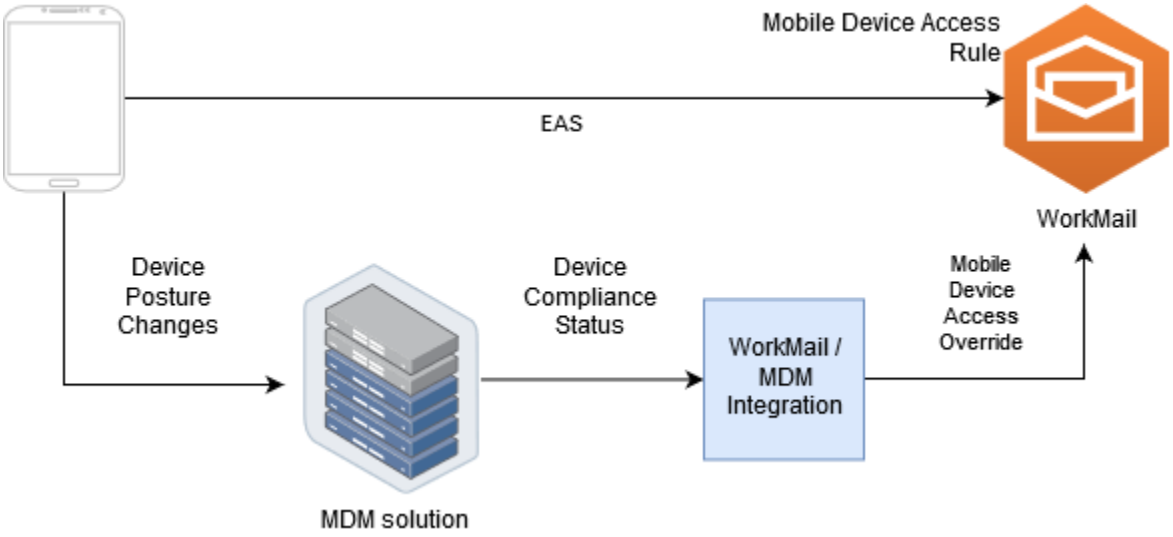
Im Proxymodus verwenden mobile Geräte das Exchange Active Sync (EAS) -Protokoll über Ihre MDM-Lösung, um auf Amazon WorkMail zuzugreifen. Die MDM-Lösung verwendet die Geräteposition, um den Zugriff auf WorkMail Amazon-Daten zuzulassen oder zu verweigern. Verwenden Sie auf WorkMail Amazon-Seite eine Zugriffskontrollregel, die den EAS-Zugriff nur von der oder den IP-Adressen der MDM-Lösung aus erlaubt. Weitere Informationen finden Sie unter Arbeiten mit Zugriffskontrollregeln.

Die folgende Abbildung zeigt eine typische Konfiguration im Proxymodus.



Im Direktmodus verwenden Mobilgeräte EAS, um WorkMail direkt auf Amazon zuzugreifen. Ihre MDM-Lösung empfängt Änderungen des Gerätestatus und bewertet kontinuierlich, ob jedes Gerät diese Anforderungen erfüllt. Wenn die MDM-Lösung feststellt, dass sich die Systemeinstellungen ändern, z. B. wenn ein Gerät nicht mehr richtlinientreu ist, kann sie verschiedene Maßnahmen ergreifen und sendet in der Regel Benachrichtigungen oder Ereignisse aus. Ein WorkMail Amazon-Administrator kann ein System einrichten, das diese Compliance-Status-Ereignisse abhört und automatisch Überschreibungen für den Zugriff auf mobile Geräte erstellt, die den Zugriff auf Geräte ermöglichen oder verweigern, wenn diese die MDM-Geräteanforderungen erfüllen oder nicht.

Die folgende Abbildung zeigt eine typische Konfiguration im Direktmodus.



Konfiguration einer WorkMail Organisation für die Integration mit einer MDM-Lösung eines Drittanbieters im Direktmodus

Für die Integration mit einer MDM-Lösung (Mobile Device Management) eines Drittanbieters im Direktmodus müssen Sie die folgenden Anforderungen erfüllen:

- Erstellen Sie Zugriffskontrollregeln, die den Zugriff auf Benutzergeräte nur auf das ActiveSync Protokoll beschränken.
- Erstellen Sie eine Standardregel für den Zugriff auf mobile Geräte deny-to-all "", um sicherzustellen, dass allen unbekannten oder nicht verwalteten Mobilgeräten standardmäßig verweigert wird.
- Verwenden Sie eine Lösung für die Verwaltung mobiler Geräte, die benutzerdefinierte Benachrichtigungen oder Ereignisse ausgibt, wenn sich die Sicherheitslage eines Geräts ändert, d. h., dass es die Richtlinien erfüllt oder nicht.
- Erstellen Sie eine benutzerdefinierte Softwarekomponente, um diese Benachrichtigungen abzuhören, und rufen Sie das Amazon WorkMail SDK auf, um Überschreibungen für den Zugriff auf mobile Geräte zu erstellen.

Diese Komponenten stellen sicher, dass alle Benutzergeräte ihre MDM-Konformitätsanforderungen erfüllen, bevor sie auf ihre WorkMail Amazon-Postfächer zugreifen dürfen.

Verwenden Sie Zugriffskontrollregeln, um den Zugriff von Mobilgeräten auf zu beschränken ActiveSync

Sie müssen sicherstellen, dass alle Geräte nur das ActiveSync Protokoll verwenden, und Sie können dazu Zugriffskontrollregeln verwenden. Beispielsweise können Sie den Zugriff auf andere E-Mail-Protokolle nur von einem internen IP-Adressbereich aus gewähren und dann nur zulassen, ActiveSync wenn Sie von außerhalb der Unternehmensfirewall auf E-Mails zugreifen. Sie müssen dies tun, da Sie Geräte nur anhand einer Geräte-ID identifizieren ActiveSync können. Sie können keine Protokolle wie das Internet Message Access Protocol (IMAP) oder Exchange Web Services verwenden. Weitere Informationen finden Sie unter Arbeiten mit Zugriffssteuerungsregeln.

Erstellen Sie eine Standardzugriffsregel „Allen verweigern“

Um alle Entscheidungen über den Zugriff auf mobile Geräte auf die Verwaltungslösung für mobile Geräte eines Drittanbieters zu übertragen, erstellen Sie eine Zugriffsregel, die automatisch alle Geräte verweigert, sofern sie nicht pro Benutzer oder pro Gerät außer Kraft gesetzt wird. Weitere Informationen finden Sie unter Zugriffsregeln für mobile Geräte verwalten.

Dieses Beispiel zeigt eine Regel „Allen verweigern“.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

Reagieren Sie auf Änderungen der Gerätehaltung und erstellen Sie Überschreibungen für den Zugriff auf mobile Geräte

Sie müssen Ihre MDM-Lösung so konfigurieren, dass Benachrichtigungen über Änderungen der Gerätehaltung gesendet werden. Diese Benachrichtigungen müssen von einer Komponente verarbeitet werden, die das Amazon WorkMail SDK verwenden kann, um Zugriffsüberschreibungen für mobile Geräte zu erstellen oder zu aktualisieren. Standardmäßig WorkMail verweigert Amazon den Zugriff auf nicht verwaltete oder neu bereitgestellte Geräte aufgrund der Standardregel „Allen verweigern“ für den Zugriff auf mobile Geräte, die weiter oben in diesem Thema beschrieben wurde. Wenn die MDM-Lösung feststellt, dass das Gerät alle Anforderungen erfüllt, und eine Benachrichtigung ausgibt, die darauf hinweist, dass das Gerät konform ist, kann diese Komponente auf diese Benachrichtigung reagieren, indem sie eine Überschreibung des Zugriffs auf mobile Geräte mit Wirkung von `ALLOW` für den angegebenen Benutzer und das angegebene Gerät erstellt. Wenn das Gerät später nicht mehr richtlinientreu ist, sendet die Lösung für die Verwaltung mobiler Geräte eine weitere Benachrichtigung aus, und die Zugriffsüberschreibung kann gelöscht oder geändert werden, um dem Gerät den Zugriff zu verweigern. Weitere Informationen finden Sie unter Überschreibungen für den Zugriff auf mobile Geräte verwalten.

Ein Beispiel für die WorkMail Integration von Amazon mit MDM finden Sie in dieser AWS Beispielanwendung.

Arbeiten mit Postfachberechtigungen

Sie können Postfachberechtigungen in Amazon verwenden WorkMail , um Benutzern und Gruppen das Recht zu gewähren, in den Postfächern anderer Benutzer zu arbeiten. Postfachberechtigungen gelten für ein gesamtes Postfach. Sie ermöglichen es mehreren Benutzern, auf dasselbe Postfach zuzugreifen, ohne die Anmeldeinformationen dieses Postfachs gemeinsam zu nutzen. Benutzer mit Postfachberechtigungen können Postfachdaten lesen und ändern und E-Mails über das geteilte Postfach senden.

> **Note**
>
> Benutzer mit Berechtigungen für ein Postfach, das einem Benutzer gehört, der in der globalen Adressliste ausgeblendet ist, können trotzdem auf das Postfach des verborgenen Benutzers zugreifen.

In der folgenden Liste sind die Berechtigungen erhalten, die Sie erteilen können:

- Vollzugriff — Ermöglicht vollen Lese- und Schreibzugriff auf das Postfach, einschließlich der Berechtigungen zum Ändern von Berechtigungen auf Ordnerebene.

  > **Note**
  >
  > Diese Option ist nur für Benutzer verfügbar. Gruppen können keine vollen Zugriffsrechte gewährt werden.

- Im Namen senden — Ermöglicht es einem Benutzer oder einer Gruppe, E-Mails im Namen eines anderen Benutzers zu senden. Der Postfachbesitzer wird in der Kopfzeile From: (Von) und der Sender in der Kopfzeile Sender: (Absender) angezeigt.
- Senden als — Ermöglicht es einem Benutzer oder einer Gruppe, als Postfachbesitzer E-Mails zu senden, ohne dass der tatsächliche Absender der Nachricht angezeigt wird. Der Postfachbesitzer wird in den Kopfzeilen From: (Von) und Sender: (Absender) angezeigt.
- Keine — Hindert einen Benutzer oder eine Gruppe daran, E-Mails zu senden.

> **Note**
>
> Wenn Sie Postfachberechtigungen für eine Gruppe gewähren, werden diese Berechtigungen auf alle Mitglieder der Gruppe ausgedehnt, einschließlich der Mitglieder verschachtelter Gruppen.

Wenn Sie Postfachberechtigungen gewähren, aktualisiert der WorkMail AutoDiscover Amazon-Service automatisch den Zugriff auf diese Postfächer für die Benutzer oder Gruppen, die Sie hinzugefügt haben.

Beim Microsoft Outlook-Client in Windows können Benutzer mit vollständigen Zugriffsberechtigungen automatisch auf freigegebene Postfächer zugreifen. Warten Sie bis zu 60 Minuten, bis die Änderungen übernommen wurden, und starten Sie dann Microsoft Outlook neu.

Für die WorkMail Amazon-Webanwendung und andere E-Mail-Clients können Benutzer mit vollen Zugriffsberechtigungen die gemeinsam genutzten Postfächer manuell öffnen. Geöffnete Postfächer bleiben auch zwischen Sitzungen geöffnet, sofern der Benutzer diese nicht schließt.

Themen

- Über Postfach- und Ordnerberechtigungen
- Verwaltung der Postfachberechtigungen für Benutzer
- Verwaltung von Postfachberechtigungen für Gruppen

Über Postfach- und Ordnerberechtigungen

Postfachberechtigungen gelten für alle Ordner innerhalb eines Postfachs. Diese Berechtigungen können nur vom AWS Kontoinhaber oder einem IAM-Benutzer aktiviert werden, der berechtigt ist, die Amazon WorkMail Management API aufzurufen. Verwenden Sie die oder die WorkMail Amazon-API, um Berechtigungen für Postfächer oder für Gruppen als Ganzes festzulegen und zu ändern. AWS Management Console Sie können bis zu 100 Postfach- und Gruppenberechtigungen über die Konsole verwalten. Verwenden Sie die WorkMail Amazon-API, um Berechtigungen für mehr Benutzer und Gruppen zu verwalten.

Ordnerberechtigungen gelten nur für einen einzigen Ordner. Endbenutzer können Ordnerberechtigungen mithilfe eines E-Mail-Clients oder mithilfe der WorkMail Amazon-Webanwendung festlegen. Weitere Informationen zur Nutzung der WorkMail Amazon-

Webanwendung zum Teilen von Ordnern finden Sie unter Ordner teilen und Ordnerberechtigungen im WorkMail Amazon-Benutzerhandbuch.

Verwaltung der Postfachberechtigungen für Benutzer

Sie können die WorkMail Amazon-Konsole verwenden, um Postfachberechtigungen für Benutzer und Gruppen zu verwalten. In den folgenden Abschnitten wird erklärt, wie die Berechtigungen für Benutzer verwaltet werden. Informationen zur Verwaltung von Berechtigungen für Gruppen finden Sie unterVerwaltung von Postfachberechtigungen für Gruppen.

Themen

- Hinzufügen von Berechtigungen
- Postfachberechtigungen für Benutzer bearbeiten

Hinzufügen von Berechtigungen

Wenn Sie Berechtigungen hinzufügen, gewähren Sie einem Benutzer das Recht, eine oder mehrere Aufgaben im Postfach eines anderen Benutzers auszuführen. Angenommen, Mitarbeiter A muss Nachrichten im Namen seines Vorgesetzten, Mitarbeiter B, senden. Um diese Berechtigung zu erteilen, gehen Sie zu den Postfacheinstellungen von Mitarbeiter B und erteilen Mitarbeiter A die Erlaubnis, die angeforderte Aufgabe auszuführen.

Um Postfachberechtigungen hinzuzufügen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region. Wählen Sie in der Navigationsleiste die Region aus, die Ihren Anforderungen entspricht. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, für die Sie Berechtigungen verwalten möchten.
3. Wählen Sie im Navigationsbereich Benutzer und dann den Namen des Benutzers aus, für den Sie Berechtigungen verwalten möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) und anschließend die Option Add Permissions (Berechtigung hinzufügen).

   Das Dialogfeld „Berechtigungen hinzufügen“ wird angezeigt.

5. Öffnen Sie die Liste Neue Berechtigungen hinzufügen und wählen Sie den Benutzer oder die Gruppe aus, die Zugriff auf das Postfach benötigt.
6. Wählen Sie unter Postfachberechtigungen und Sendeberechtigungen die gewünschten Optionen aus.
7. Wählen Sie Hinzufügen aus.

Es kann bis zu fünf Minuten dauern, bis neue Berechtigungen an Benutzer weitergegeben werden.

Postfachberechtigungen für Benutzer bearbeiten

Wenn Sie Postfachberechtigungen für einen Benutzer bearbeiten, ändern Sie den Zugriff, den andere Benutzer auf das Postfach dieses Benutzers haben. Durch das Bearbeiten von Postfachberechtigungen wird der Zugriff für den ursprünglichen Benutzer des Postfachs nicht geändert.

So bearbeiten Sie Postfachberechtigungen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region. Wählen Sie in der Navigationsleiste die Region aus, die Ihren Anforderungen entspricht. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, für die Sie Berechtigungen verwalten möchten.
3. Wählen Sie im Navigationsbereich Benutzer und dann den Namen des Benutzers aus, dessen Berechtigungen Sie bearbeiten möchten.
4. Wählen Sie die Registerkarte Berechtigungen.

   Eine Liste der Benutzer und Gruppen, die Zugriff auf das Postfach haben, wird angezeigt.
5. Wählen Sie das Optionsfeld neben dem Benutzer oder der Gruppe aus, den bzw. die Sie ändern möchten, und führen Sie dann eine der folgenden Aktionen aus:

   Um die Berechtigungen eines Benutzers zu entfernen

   1. Wählen Sie Remove (Entfernen) aus.

      Das Dialogfeld „Berechtigungen entfernen“ wird angezeigt.
   2. Wählen Sie im Dialogfeld „Berechtigungen entfernen“ die Option „Entfernen“ aus.

Um die Berechtigungen eines Benutzers zu bearbeiten

1. Wählen Sie Edit (Bearbeiten) aus.

   Das Dialogfeld „Berechtigungen bearbeiten“ wird angezeigt.
2. Legen Sie die Berechtigungen nach Bedarf fest und wählen Sie dann Speichern.

Um einem anderen Benutzer Berechtigungen für das Postfach zu gewähren

1. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.

   Das Dialogfeld „Berechtigungen hinzufügen“ wird angezeigt.
2. Öffnen Sie die Liste Neue Berechtigungen hinzufügen und wählen Sie den Benutzer aus, den Sie hinzufügen möchten.
3. Legen Sie die Berechtigungen nach Bedarf fest und wählen Sie dann Hinzufügen aus.

Es kann bis zu fünf Minuten dauern, bis Änderungen an den Berechtigungen an die Benutzer weitergegeben werden.

Verwaltung von Postfachberechtigungen für Gruppen

Sie können Gruppenberechtigungen für Amazon hinzufügen oder entfernen WorkMail.

> **Note**
>
> Sie können einer Gruppe keine Vollzugriffsberechtigungen zuweisen, da Gruppen kein Postfach haben, auf das sie zugreifen können.

So verwalten Sie Gruppenberechtigungen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie bei Bedarf die Option AWS-Region In der Leiste oben im Konsolenfenster, öffnen Sie die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.

2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus, für die Sie Berechtigungen verwalten möchten.
3. Wählen Sie im Navigationsbereich Gruppen und dann den Namen der Gruppe aus, für die Sie Berechtigungen festlegen möchten.
4. Wählen Sie die Registerkarte „Berechtigungen“ und anschließend „Berechtigungen hinzufügen“ aus.

   Das Dialogfeld „Berechtigungen hinzufügen“ wird angezeigt.
5. Öffnen Sie die Liste Neue Berechtigungen hinzufügen und wählen Sie den Benutzer oder die Gruppe aus, dem bzw. der Sie Berechtigungen für das Postfach gewähren möchten.
6. Wählen Sie unter Postfachberechtigungen und Sendeberechtigungen die gewünschten Optionen aus.
7. Wählen Sie Hinzufügen aus.

Es kann bis zu fünf Minuten dauern, bis Änderungen an Berechtigungen an die Benutzer weitergegeben werden.

Programmatischer Zugriff auf Postfächer

Verwenden Sie das Exchange Web Services (EWS) WorkMail -Protokoll, um programmgesteuert auf Amazon-Postfächer zuzugreifen. Mit EWS können Sie auf alle Elementtypen in einem Postfach zugreifen. Hier sind einige EWS-Bibliotheken, die Sie mit Amazon verwenden können WorkMail:

- Java — EWS-Java-API
- .Net — Von EWS verwaltete API
- Python — ExchangeLib

Amazon unterstützt WorkMail auch IMAP- und SMTP-Protokolle, mit denen Sie E-Mails senden und empfangen können. Die für Amazon URLs unterstützten WorkMail Protokolle finden Sie unter WorkMailAmazon-Endpunkte und Kontingente.

Bei Verwendung des EWS-Protokolls WorkMail unterstützt Amazon die folgenden Authentifizierungsmethoden:

- Standardauthentifizierung — Bei der Standardauthentifizierung geben Sie eine E-Mail-Adresse und ein Passwort ein.
- Identitätswechselrollen — Mit Identitätswechselrollen greifen Sie auf die Postfächer von Benutzern zu, ohne die Anmeldeinformationen des Benutzers eingeben zu müssen.

Themen

- Verwaltung von Identitätswechselrollen
- Verwenden von Rollen mit Identitätswechsel

Verwaltung von Identitätswechselrollen

Mit Identitätswechselrollen konfigurieren Administratoren den programmatischen Zugriff auf Benutzerpostfächer, ohne die Anmeldeinformationen des Benutzers eingeben zu müssen. Dienste und Tools können die Rolle eines Identitätswechsels übernehmen, um Aktionen in den Postfächern von Benutzern auszuführen. Identitätswechsel werden nur mit dem EWS-Protokoll unterstützt.

Überblick über die Rollen beim Identitätswechsel

Um Identitätswechsel zuzulassen, müssen Administratoren eine Identitätswechselrolle mit den folgenden Eigenschaften erstellen:

- Rollentyp — Wählen Sie entweder Vollzugriff oder Schreibgeschützt. Der Rollentyp schränkt die Art der Operationen ein, die eine Rolle ausführen kann.
- Regeln — Eine Liste von Regeln, die definieren, für welche Benutzer sich die Identitätswechselrolle ausgeben kann.

Amazon WorkMail bewertet die Regeln unter den folgenden Bedingungen:

- Wenn eine DENY-Regel zutrifft, lehnt die Richtlinie den Identitätswechsel ab. DENY-Regeln haben Vorrang vor allen ALLOW-Regeln.
- Wenn mindestens eine ALLOW-Regel zutrifft und keine DENY-Regel zutrifft, erlaubt die Richtlinie den Identitätswechsel.
- Wenn keine Regel gilt, wird der Identitätswechsel verweigert.

> **Note**
>
> Um allen Benutzern in einer WorkMail Amazon-Organisation den Identitätswechsel zuzulassen, erstellen Sie eine Regel mit dem ALLOW-Effekt und ohne Bedingungen.

> **Warning**
>
> Sie müssen Regeln erstellen, damit eine Identitätswechselrolle die Identität eines Benutzers annehmen kann. Wenn Sie keine Regeln angeben, kann eine Identitätswechselrolle nicht die Zugriffsrechte eines Benutzers übernehmen.

Nachdem die Identitätswechselrolle erstellt wurde, können Sie sie verwenden, um Zugriff auf die Postfächer der Benutzer zu erhalten. Weitere Informationen finden Sie unter Verwenden von Rollen mit Identitätswechsel.

Sicherheitsüberlegungen

Die Verwendung von Identitätswechselrollen kann zu Sicherheitsproblemen innerhalb Ihrer WorkMail Amazon-Organisation führen und. AWS-Konto Hier sind einige der potenziellen Probleme, die Sie bei der Erstellung einer Identitätswechselrolle berücksichtigen sollten:

- Transitive Berechtigungen — Wenn Benutzer A Zugriff auf das Postfach von Benutzer B hat und eine Identitätswechselrolle berechtigt ist, sich als Benutzer A auszugeben, kann diese Identitätswechselrolle die Zugriffsberechtigungen von Benutzer A annehmen und auf das Postfach von Benutzer B zugreifen.
- Zugriffskontrolle — Sie können Zugriffskontrollregeln verwenden, um den Zugriff auf eine Impersonationsrolle einzuschränken. Weitere Informationen finden Sie unter Arbeiten mit Zugriffssteuerungsregeln.
- IAM-Richtlinie — Mithilfe der Bedingung können Sie einer bestimmten WorkMail Amazon-Organisation und einer bestimmten Impersonationsrolle eine `AssumeImpersonationRole` Aktion zuweisen. `workmail:ImpersonationRoleId` Ein Beispiel für eine IAM-Richtlinie finden Sie unter. So WorkMail arbeitet Amazon mit IAM

Rollen mit Identitätswechsel erstellen

Sie können Impersonationsrollen von der WorkMail Amazon-Konsole aus erstellen.

Um eine Impersonationsrolle zu erstellen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region. Wählen Sie in der Navigationsleiste die Region aus, die Ihren Anforderungen entspricht. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus.
3. Wählen Sie Rollen mit Identitätswechsel und anschließend Rolle erstellen aus.
4. Das Dialogfeld „Identitätswechselrolle erstellen“ wird angezeigt. Geben Sie unter Rolle die folgenden Informationen ein:

   - Name — Geben Sie einen eindeutigen Namen für die Identitätswechselrolle ein.
   - (Optional) Beschreibung — Geben Sie eine Beschreibung für die Identitätswechselrolle ein.
   - Rollentyp — Wählen Sie Schreibgeschützt oder Vollzugriff.

5. Wählen Sie unter Regeln die Option Regel hinzufügen aus.
6. Das Dialogfeld Regel hinzufügen wird angezeigt. Geben Sie die folgenden Informationen ein:
   - Name — Geben Sie einen eindeutigen Namen für die Regel ein.
   - (Optional) Beschreibung — Geben Sie eine Beschreibung für die Regel ein.
   - Wählen Sie unter Wirkung die Option Zulassen oder Verweigern aus. Dies ermöglicht oder verweigert den Zugriff auf der Grundlage der Bedingungen, die Sie im folgenden Schritt auswählen.
   - (Optional) Wählen Sie unter Diese Regel: die Option Entspricht Anfragen, die sich als die ausgewählten Benutzer ausgeben, aus, um bestimmte Benutzer einzubeziehen. Wählen Sie Entspricht Anfragen, die sich als andere Benutzer als die ausgewählten Benutzer ausgeben, aus, um andere Benutzer als die ausgewählten Benutzer hinzuzufügen.
7. Wählen Sie Regel hinzufügen aus.

   > **Note**
   >
   > Regeln werden nur gespeichert, wenn Sie die entsprechende Rolle speichern.

8. Wählen Sie Rolle erstellen.

Rollen mit Identitätswechsel bearbeiten

Sie können Impersonationsrollen von der WorkMail Amazon-Konsole aus bearbeiten.

Um eine Impersonationsrolle zu bearbeiten

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region. Wählen Sie in der Navigationsleiste die Region aus, die Ihren Anforderungen entspricht. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus.
3. Wählen Sie Impersonationsrollen aus.
4. Wählen Sie den Namen der Impersonationsrolle aus, den Sie bearbeiten möchten, und klicken Sie dann auf Bearbeiten.

5. Das Dialogfeld „Identitätswechselrolle bearbeiten“ wird angezeigt. Geben Sie unter Rolle die folgenden Informationen ein:

   - Name — Geben Sie einen eindeutigen Namen für die Identitätswechselrolle ein.
   - (Optional) Beschreibung — Geben Sie eine Beschreibung für die Identitätswechselrolle ein.
   - Rollentyp — Um der Identitätswechselrolle nur Lesezugriff auf das Postfach eines Benutzers zu gewähren, wählen Sie Schreibgeschützt aus. Um der Impersonationsrolle Rechte zum Lesen und Ändern von Elementen im Postfach eines Benutzers zu gewähren, wählen Sie Vollzugriff.

6. Wählen Sie unter Regeln die Regel aus, die Sie bearbeiten möchten, und wählen Sie Bearbeiten aus.
7. Das Dialogfeld Regel bearbeiten wird angezeigt. Geben Sie die folgenden Informationen ein:

   - Name — Bearbeiten Sie den Namen der Regel.
   - (Optional) Beschreibung — Aktualisieren Sie die Regel oder geben Sie eine Beschreibung ein.
   - Wählen Sie unter Wirkung die Option Zulassen aus, um den Zugriff zuzulassen, wenn die in den Regeln festgelegten Bedingungen erfüllt sind. Um den Zugriff zu verweigern, wählen Sie Verweigern.
   - (Optional) Wählen Sie unter Diese Regel: die Option Stimmt mit Anfragen überein, die sich als die ausgewählten Benutzer ausgeben, um bestimmte Benutzer einzubeziehen. Wählen Sie Entspricht Anfragen, die sich als andere Benutzer als die ausgewählten Benutzer ausgeben, aus, um andere Benutzer als die ausgewählten Benutzer hinzuzufügen.

8. Wählen Sie Save (Speichern) aus.
9. Wählen Sie Änderungen speichern.

> **Important**
>
> Wenn Sie eine Regel für den Identitätswechsel ändern, kann die Aktualisierung der betroffenen Postfächer bis zu fünf Minuten dauern. Während der Regelaktualisierung stellen Sie möglicherweise ein inkonsistentes Verhalten in Ihrem Postfach fest. Wenn Sie jedoch eine Rolle testen, WorkMail reagiert Amazon auf der Grundlage der aktualisierten Regel erwartungsgemäß. Weitere Informationen finden Sie unter Testen von Rollen mit Identitätswechsel.

Testen von Rollen mit Identitätswechsel

Sie können eine Identitätswechselrolle von der WorkMail Amazon-Konsole aus testen.

Um eine Impersonationsrolle zu testen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region. Wählen Sie in der Navigationsleiste die Region aus, die Ihren Anforderungen entspricht. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus.
3. Wählen Sie Impersonationsrollen aus.
4. Wählen Sie die Impersonationsrolle aus, die Sie testen möchten.
5. Wählen Sie „Rolle testen“ aus.
6. Das Dialogfeld „Rolle mit Identitätswechsel testen“ wird angezeigt. Wählen Sie unter Zielbenutzer den Benutzer aus, für den Sie den Identitätswechselzugriff testen möchten.
7. Wählen Sie Test aus.

Impersonationsrollen löschen

Sie können eine Impersonationsrolle von der WorkMail Amazon-Konsole löschen.

Um eine Impersonationsrolle zu löschen

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie, falls erforderlich, die Region. Wählen Sie in der Navigationsleiste die Region aus, die Ihren Anforderungen entspricht. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen der Organisation aus.
3. Wählen Sie Impersonationsrollen aus.
4. Wählen Sie den Namen der Impersonationsrolle aus, die Sie löschen möchten.
5. Wählen Sie Löschen.
6. Das Dialogfeld „Rolle löschen“ wird angezeigt. Um das Löschen zu bestätigen, geben Sie den Namen der Rolle in das Dialogfeld ein und wählen Sie Löschen.

Verwenden von Rollen mit Identitätswechsel

Verwenden Sie die WorkMail Amazon-API-Aktion, um auf Postfachdaten zuzugreifen`AssumeImpersonationRole`. Weitere Informationen zu Amazon WorkMail APIs finden Sie unter API-Referenz.

`AssumeImpersonationRole`gibt a zurück`Token`. Dies `Token` muss innerhalb von 15 Minuten über den HTTP-Header an das EWS-Protokoll übergeben `Authorization` werden.

Die folgenden Beispiele zeigen, wie Identitätswechselrollen mit dem EWS-Protokoll verwendet werden können. Die in den Beispielen verwendeten Konstanten geben die folgenden Details an, die nur für Ihre Organisation und Ihr Konto gelten:

- *`WORKMAIL_ORGANIZATION_ID`*— WorkMail Amazon-Organisations-ID
- *`IMPERSONATION_ROLE_ID`*— ID der Rolle beim Identitätswechsel
- *`WORKMAIL_EWS_URL`*— EWS-Endpunkt an WorkMail Amazon-Endpunkten und Kontingenten verfügbar
- *`EMAIL_ADDRESS`*— E-Mail-Adresse des Benutzerpostfachs

Example Java — EWS-Java-API

```
import software.amazon.awssdk.services.workmail.WorkMailClient;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleRequest;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleResponse;

import microsoft.exchange.webservices.data.core.ExchangeService;
import microsoft.exchange.webservices.data.core.enumeration.misc.ExchangeVersion;
import microsoft.exchange.webservices.data.misc.ImpersonatedUserId;
import microsoft.exchange.webservices.data.core.enumeration.misc.ConnectingIdType;

// ...

AssumeImpersonationRoleResponse response = workMailClient.assumeImpersonationRole(
    AssumeImpersonationRoleRequest.builder()
        .organizationId(WORKMAIL_ORGANIZATION_ID)
        .impersonationRoleId(IMPERSONATION_ROLE_ID)
        .build());

ExchangeService exchangeService = new
 ExchangeService(ExchangeVersion.Exchange2010_SP2);
```

```
exchangeService.setUrl(URI.create(WORKMAIL_EWS_URL));
exchangeService.getHttpHeaders().put("Authorization", "Bearer " + response.token());
exchangeService.setImpersonatedUserId(new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS));
```

Example .Net — Von EWS verwaltete API

```
using Amazon.WorkMail;
using Amazon.WorkMail.Model;

using Microsoft.Exchange.WebServices.Data;

// ...

AssumeImpersonationRoleRequest request = new AssumeImpersonationRoleRequest();
request.OrganizationId = WORKMAIL_ORGANIZATION_ID;
request.ImpersonationRoleId = IMPERSONATION_ROLE_ID;
AssumeImpersonationRoleResponse response =
 workMailClient.AssumeImpersonationRole(request);

ExchangeService service = new ExchangeService(ExchangeVersion.Exchange2010_SP2);
service.Url = new Uri(WORKMAIL_EWS_URL);
service.HttpHeaders.Add("Authorization", "Bearer " + response.Token);
service.ImpersonatedUserId = new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS);
```

Example Python — ExchangeLib

```
import boto3

from requests.auth import AuthBase
from exchangelib.transport import AUTH_TYPE_MAP
from exchangelib import Configuration, Account, Version, IMPERSONATION
from exchangelib.version import EXCHANGE_2010_SP2


work_mail_client = boto3.client("workmail")

class ImpersonationRoleAuth(AuthBase):
    def __init__(self):
         self.token = work_mail_client.assume_impersonation_role(
             OrganizationId=WORKMAIL_ORGANIZATION_ID,
             ImpersonationRoleId=IMPERSONATION_ROLE_ID
```

```
        )["Token"]

    def __call__(self, r):
        r.headers["Authorization"] = "Bearer " + self.token
        return r

AUTH_TYPE_MAP["ImpersonationRoleAuth"] = ImpersonationRoleAuth

ews_config = Configuration(
    service_endpoint=WORKMAIL_EWS_URL,
    version=Version(build=EXCHANGE_2010_SP2),
    auth_type="ImpersonationRoleAuth"
)
ews_account = Account(
    config=ews_config,
    primary_smtp_address=EMAIL_ADDRESS,
    access_type=IMPERSONATION
)
```

Postfachinhalt exportieren

Verwenden Sie die StartMailboxExportJobAPI-Aktion in der Amazon WorkMail API-Referenz, um WorkMail Amazon-Postfachinhalte in einen Amazon Simple Storage Service (Amazon S3) -Bucket zu exportieren. Diese Aktion exportiert alle E-Mail-Nachrichten und Kalendereinträge aus dem angegebenen Postfach in eine `.zip` Datei im Amazon S3 S3-Bucket im MIME-Format. Andere Elemente, wie Kontakte und Aufgaben, werden nicht exportiert.

Wie lange es dauert, bis der Postfachexport abgeschlossen ist, hängt von der Größe und Anzahl der Elemente im Postfach ab. Da der Postfachexportauftrag über einen bestimmten Zeitraum stattfindet, stellt er keine Momentaufnahme des Postfachinhalts zu einem bestimmten Zeitpunkt dar. Um den Status eines Exportauftrags zu sehen, verwenden Sie die ListMailboxExportJobsAPI-Aktionen DescribeMailboxExportJoboder in der Amazon WorkMail API-Referenz.

Wenn ein Postfach-Exportauftrag abgeschlossen ist, wird die `.zip` Datei im Amazon S3 S3-Bucket mit dem von Ihnen angegebenen symmetrischen AWS Key Management Service (AWS KMS) Customer Master Key (CMK) verschlüsselt. Da die AWS KMS Verschlüsselung in Amazon S3 integriert ist, sind die entschlüsselten Daten für den Benutzer sichtbar, der sie herunterlädt, solange der Benutzer Zugriff auf das AWS KMS CMK hat.

Voraussetzungen

Für den Export von Postfachinhalten gelten folgende Voraussetzungen:

- Die Fähigkeit zu programmieren.
- Ein WorkMail Amazon-Administratorkonto.
- Ein Amazon S3 S3-Bucket, der keinen öffentlichen Zugriff erlaubt. Weitere Informationen finden Sie unter Blockieren des öffentlichen Zugriffs mit Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch und im Amazon Simple Storage Service-Benutzerhandbuch.
- Ein symmetrisches AWS KMS CMK. Weitere Informationen finden Sie unter Erste Schritte im AWS Key Management Service -Entwicklerhandbuch.
- Eine AWS Identity and Access Management (IAM-) Rolle mit einer Richtlinie, die die Erlaubnis erteilt, in den Amazon S3 S3-Bucket zu schreiben und die gesendeten Dateien mit dem AWS KMS CMK zu verschlüsseln. Weitere Informationen finden Sie unter So WorkMail arbeitet Amazon mit IAM.

Beispiele für IAM-Richtlinien und Rollenerstellung

Das folgende Beispiel zeigt eine IAM-Richtlinie, die die Erlaubnis erteilt, in den Amazon S3 S3-Bucket zu schreiben und die gesendeten Dateien mit dem AWS KMS CMK zu verschlüsseln. Um diese Beispielrichtlinie im folgenden Beispiel: Exportieren von Postfachinhalten Verfahren zu verwenden, speichern Sie die Richtlinie als JSON-Datei mit einem Dateinamen. `mailbox-export-policy.json`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:GetBucketPolicyStatus"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/KEY-ID"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-
bucket/S3-PREFIX*"
                }
            }
        }
```

```
    ]
}
```

Das folgende Beispiel zeigt eine IAM-Vertrauensrichtlinie, die an die von Ihnen erstellte IAM-Rolle angehängt ist. Um diese Beispielrichtlinie im folgenden Beispiel: Exportieren von Postfachinhalten Verfahren zu verwenden, speichern Sie die Richtlinie als JSON-Datei mit einem Dateinamen. `mailbox-export-trust-policy.json`

Sie müssen die `aws:SourceAccount` Bedingungen `aws:SourceArn` und nicht gleichzeitig verwenden. Sie können beispielsweise `aws:SourceArn` aus der Richtlinie streichen, wenn Sie dieselbe Rolle verwenden müssen, um Nachrichten von verschiedenen WorkMail Amazon-Organisationen unter demselben AWS Konto zu exportieren. Weitere Informationen zu Bedingungsschlüsseln finden Sie in den AWS globalen Bedingungskontextschlüsseln im AWS Identity and Access Management-Benutzerhandbuch.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmail:us-east-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
        }
      }
    }
  ]
}
```

Sie können den verwenden AWS CLI , um die IAM-Rolle in Ihrem Konto zu erstellen, indem Sie die folgenden Befehle ausführen.

```
aws iam create-role --role-name WorkmailMailboxExportRole --assume-role-policy-
document file://mailbox-export-trust-policy.json --region us-east-1
```

```
aws iam put-role-policy --role-name WorkmailMailboxExportRole --policy-
name MailboxExport --policy-document file://mailbox-export-policy.json
```

Weitere Informationen zu finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

Beispiel: Exportieren von Postfachinhalten

Nachdem Sie die IAM-Rolle und die Richtlinien im vorherigen Abschnitt erstellt haben, führen Sie die folgenden Schritte aus, um Ihren Postfachinhalt zu exportieren. Sie benötigen Ihre WorkMail Amazon-Organisations- und Benutzer-ID (Entitäts-ID), auf die Sie in der WorkMail Amazon-Konsole oder über die WorkMail Amazon-API zugreifen können.

Beispiel: Um Postfachinhalte zu exportieren

1. Verwenden Sie den AWS CLI , um den Postfach-Exportauftrag zu starten.

   ```
   aws workmail start-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --entity-
   id S-1-1-11-1111111111-2222222222-3333333333-3333 --kms-key-
   arn arn:aws:kms:us-east-1:111122223333:key/KEY-ID --role-arn
    arn:aws:iam::111122223333:role/WorkmailMailboxExportRole --s3-bucket-name amzn-s3-
   demo-bucket --s3-prefix S3-PREFIX
   ```

2. Verwenden Sie den AWS CLI , um den Status der Postfach-Exportaufträge für Ihre WorkMail Amazon-Organisation zu überwachen.

   ```
   aws workmail list-mailbox-export-jobs --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56
   ```

   Verwenden Sie alternativ die vom **`start-mailbox-export-job`** Befehl generierte Job-ID, um nur den Status dieses Postfach-Exportauftrags zu überwachen.

   ```
   aws workmail describe-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
   ```

Wenn der Status des Postfach-Exportauftrags ABGESCHLOSSEN ist, sind die exportierten Postfachelemente in einer `.zip` Datei im angegebenen Amazon S3 S3-Bucket verfügbar.

Im Folgenden finden Sie ein Beispiel für das Ausgabeprotokoll des exportierten Postfachs:

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportableElemente wie Notizen und Kontakte werden nicht unterstützt.

Überlegungen

Beim Exportieren von Postfachaufträgen für Amazon gelten die folgenden Überlegungen WorkMail:

- Sie können bis zu 10 Postfach-Exportaufträge gleichzeitig für eine bestimmte WorkMail Amazon-Organisation ausführen.
- Sie können einen Postfach-Exportauftrag für ein bestimmtes Postfach bis zu einmal alle 24 Stunden ausführen.
- Die folgenden Ressourcen müssen sich alle in derselben AWS Region befinden:
  - WorkMail Amazon-Organisation
  - AWS KMS CMK
  - Amazon-S3-Bucket

Fehlerbehebung

In den Themen in diesem Abschnitt wird erklärt, wie Sie Probleme in Amazon beheben können WorkMail.

Themen

- Viewing email headers
- E-Mail-Weiterleitung

Viewing email headers

Die Informationen in den E-Mail-Headern können Ihnen bei der Behebung häufiger E-Mail-Probleme von Benutzern helfen. Amazon WorkMail ermöglicht es Ihnen, die Header-Informationen für jede Nachricht einzusehen.

So zeigen Sie E-Mail-Header in Amazon an WorkMail

1. Doppelklicken Sie in der WorkMail Amazon-Webanwendung auf die E-Mail-Nachricht, um sie zu öffnen.
2. Wählen Sie Nachrichtenoptionen (das Zahnrad- und Umschlagsymbol) in der oberen rechten Ecke der Nachricht neben dem Datum „Gesendet am“.

The email headers appear under Internet Headers.

E-Mail-Weiterleitung

Wenn ein Benutzer keine E-Mails mehr erhält, hat Ihre WorkMail Amazon-Organisation möglicherweise ein Problem mit der E-Mail-Weiterleitung. In den Schritten in diesem Abschnitt werden gängige Methoden zur Lösung von Zustell- und Weiterleitungsproblemen erläutert.

Probleme mit eingehenden E-Mails:

- Überprüfen Sie den MX-Eintrag für die Domain, die mit Ihrer WorkMail Amazon-Organisation verknüpft ist. `WorkMail`sollte der einzige Eintrag sein und sollte die niedrigste Priorität haben. Mehrere MX-Einträge können dazu führen, dass der falsche Dienst Nachrichten empfängt. Weitere Hinweise zu MX-Einträgen finden Sie unterVerifizieren von Domänen.

- Überprüfen Sie die Einstellungen für Domain-based Message Authentication, Reporting and Conformance (DMARC) für Ihr Unternehmen in der Amazon-Konsole. WorkMail DMARC-Einträge werden zum Schutz vor häufigen Angriffen wie Spoofing oder Phishing verwendet, die die Kontoanmeldeinformationen eines Benutzers gefährden können. Weitere Informationen zu DMARC finden Sie unter. Durchsetzen von DMARC-Richtlinien für eingehende E-Mails
- Überprüfen Sie die Amazon Simple Email Service-Regel für eingehende Nachrichten. Wenn die Regel andere Aktionen als Amazon enthält WorkMail, können diese Aktionen fehlschlagen und dazu führen, dass Amazon WorkMail keine E-Mails mehr empfängt. Weitere Informationen zu den Amazon SES SES-Regeln finden Sie unter Integrate with Amazon WorkMail Action im Amazon Simple Email Service Developer Guide.
- Aktivieren Sie die Nachrichtenverfolgung in Amazon WorkMail und überprüfen Sie dann die Protokolle auf Zustellungsprobleme. Weitere Informationen zur Nachrichtenverfolgung finden Sie unterDie Protokollierung von E-Mail-Ereignissen aktivieren.

Probleme mit ausgehenden E-Mails

- Stellen Sie sicher, dass Ihr SPF-Eintrag Amazon SES enthält. Überprüfen Sie die Domains-Seite in der WorkMail Amazon-Konsole, um dies zu überprüfen. Weitere Informationen zu SPF finden Sie unterAuthentifizierung Ihrer E-Mails mit SPF.
- Stellen Sie sicher, WorkMail dass Amazon über die Berechtigungen zur Nutzung der Domain verfügt. Wenn nicht, fügen Sie die Domain erneut hinzu. Hinzufügen einer DomäneIn diesem Handbuch finden Sie die Anleitungen.

E-Mail-Journaling mit Amazon verwenden WorkMail

Sie können Ihre E-Mail-Kommunikation mithilfe von integrierten Archivierungs- und E-Discovery-Tools von Drittanbietern in einem E-Mail-Journal aufzeichnen. Auf diese Weise stellen Sie die Einhaltung von Compliance-Vorgaben für Datenschutz, Datenspeicherung und Datensicherheit bei der E-Mail-Speicherung sicher.

Verwenden des E-Mail-Journals

Amazon WorkMail protokolliert alle E-Mail-Nachrichten, die an einen Benutzer in der angegebenen Organisation gesendet werden, sowie alle E-Mail-Nachrichten, die von Benutzern in dieser Organisation gesendet wurden. Eine Kopie aller E-Mail-Nachrichten wird an eine vom Systemadministrator angegebene Adresse in einem Format namens gesendet`journal record`. Dieses Format ist mit den E-Mail-Programmen von Microsoft kompatibel. Für die Nutzung des E-Mail-Journals fallen keine zusätzlichen Gebühren an.

Zwei E-Mail-Adressen werden für das E-Mail-Journal verwendet — eine Journal-E-Mail-Adresse und eine Berichts-E-Mail-Adresse. Bei der E-Mail-Adresse für das Journal handelt es sich um ein dediziertes Postfach oder das Gerät eines Drittanbieters in Ihrem Konto, an das die Journalberichte gesendet werden. Über die E-Mail-Adresse für den Report werden Nachrichten zu fehlerhaften Journalberichten an den Systemadministrator gesendet.

Alle Journaldatensätze werden von einer E-Mail-Adresse gesendet, die automatisch zu Ihrer Domain hinzugefügt wird und wie folgt aussieht.

```
amazonjournaling@yourorganization.awsapps.com
```

Mit dieser Adresse ist kein Postfach verknüpft, und Sie können mit diesem Namen oder dieser Adresse kein Postfach erstellen.

> **Note**
>
> Löschen Sie den folgenden Domaineintrag nicht aus der Amazon Simple Email Service (Amazon SES) -Konsole, da sonst das E-Mail-Journaling nicht mehr funktioniert.
>
> ```
> yourorganization.awsapps.com
> ```

Jede eingehende oder ausgehende E-Mail-Nachricht generiert einen Journaleintrag, unabhängig von der Anzahl der Empfänger oder Benutzergruppen. E-Mails, für die kein Journaleintrag generiert werden kann, erzeugen eine Fehlernachricht, die an die E-Mail-Adresse für den Report gesendet wird.

So aktivieren Sie das E-Mail-Journal

1. Öffnen Sie die WorkMail Amazon-Konsole unter https://console.aws.amazon.com/workmail/.

   Ändern Sie gegebenenfalls die AWS Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. For more information, see Regions and endpoints in the Allgemeine Amazon Web Services-Referenz.
2. Wählen Sie im Navigationsbereich Organizations und dann den Namen Ihrer Organisation aus.
3. Wählen Sie im Navigationsbereich unter Organisationseinstellungen die Registerkarte Journaling und dann Bearbeiten aus.
4. Stellen Sie den Schieberegler für den Journalstatus auf „Ein“.
5. Geben Sie in das Feld Journal-E-Mail-Adresse die E-Mail-Adresse ein, die Sie von Ihrem E-Mail-Journaling-Anbieter erhalten haben.

   > **Note**
   >
   > Wir empfehlen die Verwendung eines dedizierten Journal-Anbieters.
6. Geben Sie im Feld Berichts-E-Mail-Adresse die Adresse des E-Mail-Administrators ein.
7. Wählen Sie Save (Speichern) aus. Die Änderungen gelten sofort.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in den einzelnen Versionen des WorkMail Amazon-Administratorhandbuchs beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Unterstützung für die Audit-Protokollierung	Die Auditprotokolle können verwendet werden, um den Benutzerzugriff auf Postfächer zu überwachen, nach verdächtigen Aktivitäten zu suchen und Konfigurationen von Zugriffskontroll- und Verfügbarkeitsanbietern zu debuggen. Weitere Informationen finden Sie unter Aktivieren der Auditprotokollierung und Protokollierung und Überwachung in Amazon WorkMail im WorkMail Amazon-Administratorhandbuch.	20. März 2024
Unterstützung für Transport Layer Security (TLS)	Amazon hat die Unterstützung für Transport Layer Security (TLS) 1.0 und 1.1 WorkMail eingestellt. Wenn Sie TLS 1.0 oder 1.1 verwenden, müssen Sie die TLS-Version auf 1.2 aktualisieren.	2. November 2022
Entfernte Benutzer	Remote-Benutzer sind WorkMail Amazon-Benutzer, die außerhalb der WorkMail Amazon-Organisation oder auf	18. September 2023

	einer anderen E-Mail-Domain gehostet werden. Weitere Informationen finden Sie unter Benutzer im WorkMail Amazon-Administratorhandbuch.	
Programmgesteuerter Zugriff auf Postfächer	Amazon bietet WorkMail jetzt Impersonation Roles an, um programmatischen Zugriff auf Postfächer zu gewähren. Weitere Informationen finden Sie unter Programmatischer Zugriff auf Postfächer im WorkMail Amazon-Administratorhandbuch.	4. Oktober 2022
Anbieter für benutzerdefinierte Verfügbarkeit bei Amazon konfigurieren WorkMail	Amazon WorkMail unterstützt die Verwendung von Custom Availablity Providers ()CAPs. Weitere Informationen finden Sie unter Configuring a Custom Availability Provider im WorkMail Amazon-Administratorhandbuch.	30. Juni 2022
Änderungen an der Konsole beim Erstellen einer Organisation	Die WorkMail Amazon-Konsolenoberfläche zum Erstellen einer Organisation wurde aktualisiert. Weitere Informationen finden Sie unter Organisation erstellen im WorkMail Amazon-Administratorhandbuch.	23. Oktober 2020

Postfach-Inhalt exportieren	Verwenden Sie die `StartMailboxExportJob` API-Aktion, um WorkMail Amazon-Postfachinhalte in einen Amazon Simple Storage Service (Amazon S3) -Bucket zu exportieren. Weitere Informationen finden Sie unter Exportieren von Postfachinhalten im WorkMail Amazon-Administratorhandbuch.	22. September 2020
Richtlinien zur Aufbewahrung von Postfächern	Legen Sie Richtlinien zur Aufbewahrung von Postfächern für Ihre WorkMail Amazon-Organisation fest, die E-Mail-Nachrichten nach einem von Ihnen gewählten Zeitraum automatisch löschen. Weitere Informationen finden Sie unter Einrichten von Richtlinien zur Aufbewahrung von Postfächern im WorkMail Amazon-Administratorhandbuch.	28. Mai 2020
Synchrone und asynchrone Run Lambda-Aktionen	Wählen Sie synchrone oder asynchrone Konfigurationen für Lambda-Aktionen ausführen in den WorkMail Amazon-E-Mail-Flussregeln. Weitere Informationen finden Sie unter Konfiguration AWS Lambda für Amazon WorkMail im WorkMail Amazon-Administratorhandbuch.	11. Mai 2020

Arbeiten mit Zugriffskontrollregeln	Mithilfe von Zugriffskontrollregeln können WorkMail Amazon-Administratoren kontrollieren, wie auf die Postfächer ihrer Organisation zugegriffen wird. Weitere Informationen finden Sie unter Arbeiten mit Zugriffskontrollregeln im WorkMail Amazon-Administratorhandbuch.	12. Februar 2020
Eine Organisation taggen	Kennzeichnen Sie eine WorkMail Amazon-Organisation, um zwischen Organisationen in der AWS Fakturierung und Kostenmanagement Konsole zu unterscheiden oder den Zugriff auf Organisationsressourcen zu kontrollieren. Weitere Informationen finden Sie unter Organisation kennzeichnen im WorkMail Amazon-Administratorhandbuch.	23. Januar 2020
Setzen Sie DMARC-Richtlinien für eingehende E-Mails durch	Weitere Informationen finden Sie unter Durchsetzung von DMARC-Richtlinien für eingehende E-Mails im WorkMail Amazon-Administratorhandbuch.	17. Oktober 2019

Nachrichteninhalte mit Lambda abrufen	Verwenden Sie die Amazon WorkMail Message Flow API mit AWS Lambda , um Nachrichteninhalte abzurufen . Weitere Informationen finden Sie unter Abrufen von Nachrichteninhalten mit Lambda im WorkMail Amazon-Administratorhandbuch.	12. September 2019
Protokollierung Amazon WorkMail Amazon-E-Mail-Ereignissen	Aktivieren Sie die Protokollierung von E-Mail-Ereignissen in der WorkMail Amazon-Konsole, um E-Mail-Nachrichten für Ihre Organisation nachzuverfolgen. Weitere Informationen finden Sie unter Nachrichten verfolgen im WorkMail Amazon-Administratorhandbuch.	13. Mai 2019
Einfügen eines Route 53-DNS-Eintrags	Wenn Sie eine Domain einrichten, die in einer öffentlich gehosteten Route 53-Zone verwaltet wird, fügt Amazon die DNS-Einträge WorkMail automatisch für Sie ein. Weitere Informationen finden Sie unter Hinzufügen einer Domain im WorkMail Amazon-Administratorhandbuch.	13. Februar 2019

Konfiguration von Lambda für Regelaktionen für eingehende E-Mails	Amazon WorkMail unterstützt die Konfiguration von Lambda-Funktionen für die Verwendung mit Regeln für den Fluss eingehender E-Mails. Weitere Informationen finden Sie unter E-Mail-Datenflüsse verwalten im WorkMail Amazon-Administratorhandbuch.	24. Januar 2019
Lambda für Amazon WorkMail konfigurieren	Amazon WorkMail unterstützt die Konfiguration von Lambda-Funktionen für die Verwendung mit Regeln für den Fluss ausgehender E-Mails. Weitere Informationen finden Sie unter Configuring Lambda for Amazon WorkMail im Amazon WorkMail Administrator Guide.	19. November 2018
SMTP-Routing	Amazon WorkMail unterstützt die Konfiguration von SMTP-Gateways für die Verwendung mit Regeln für den Fluss ausgehender E-Mails. Weitere Informationen finden Sie unter Konfiguration von SMTP-Gateways im WorkMail Amazon-Administratorhandbuch.	1. November 2018

Debugging-Tools für benutzerdefinierte Domains	Amazon WorkMail hat Debugging-Tools für benutzerdefinierte Domains hinzugefügt. Weitere Informationen finden Sie unter Hinzufügen einer Domain im WorkMail Amazon-Administratorhandbuch.	15. Oktober 2018
Support für Outlook 2019	Amazon WorkMail unterstützt Outlook 2019 für Windows und macOS. Weitere Informationen finden Sie unter WorkMail Amazon-Systemanforderungen im WorkMail Amazon-Administratorhandbuch.	1. Oktober 2018
Verschiedene Updates	Verschiedene Updates zum Layout und zur Organisation der Themen.	12. Juli 2018
Postfachberechtigungen	Sie können Postfachberechtigungen in Amazon verwenden WorkMail , um Benutzern oder Gruppen das Recht zu gewähren, in den Postfächern anderer Benutzer zu arbeiten. Weitere Informationen finden Sie unter Arbeiten mit Postfachberechtigungen im WorkMail Amazon-Administratorhandbuch.	9. April 2018

Support für AWS CloudTrail	Amazon WorkMail ist integriert in AWS CloudTrail. Weitere Informationen finden Sie unter Protokollieren von WorkMail Amazon-API-Aufrufen mit AWS CloudTrail im WorkMail Amazon-Administratorhandbuch.	12. Dezember 2017
Support für E-Mail-Flüsse	Sie können nun Regeln für den E-Mail-Verkehr für die Bearbeitung eingehender E-Mails auf Basis der E-Mail-Adresse oder Domäne des Absenders einrichten. Weitere Informationen finden Sie unter E-Mail-Datenflüsse verwalten im WorkMail Amazon-Administratorhandbuch.	5. Juli 2017
Aktualisierungen für Quick Setup	Quick Setup erstellt jetzt ein WorkMail Amazon-Verzeichnis für Sie. Weitere Informationen finden Sie unter Amazon WorkMail mit Quick Setup einrichten im WorkMail Amazon-Administratorhandbuch.	10. Mai 2017

Support für eine breitere Palette von E-Mail-Clients	Sie können Amazon jetzt WorkMail mit Microsoft Outlook 2016 für Mac und IMAP-E-Mail-Client s verwenden. Weitere Informationen finden Sie unter Systemanforderunge n für Amazon WorkMail im WorkMail Amazon-Administrat orhandbuch.	9. Januar 2017
Support für SMTP-Journaling	Sie können Ihre E-Mail-Kommunikation in einem Journal aufzeichnen. Weitere Informationen finden Sie unter Verwenden von E-Mail-Jo urnaling mit Amazon WorkMail im WorkMail Amazon-Ad ministratorhandbuch.	25. November 2016
Support für die E-Mail-Um leitung an externe E-Mail-Ad ressen	Sie können Regeln für die E-Mail-Umleitung einrichten, indem Sie die Amazon SES SES-Identitätsrichtlinie für Ihre Domain aktualisieren. Weitere Informationen finden Sie unter Domain-Identitätsrichtlinie n bearbeiten im WorkMail Amazon-Administratorhandbuc h.	26. Oktober 2016

Support für Interoperabilität	Sie können die Interoperabilität zwischen Amazon WorkMail und Microsoft Exchange aktivieren. Weitere Informationen finden Sie unter Interoperabilität zwischen Amazon WorkMail und Microsoft Exchange im Amazon WorkMail Administrator Guide.	25. Oktober 2016
Allgemeine Verfügbarkeit	Die allgemeine Verfügbarkeitsversion von Amazon WorkMail.	4. Januar 2016
Support bei der Reservierung von Ressourcen	Unterstützung für Ressourcenreservierung, wie z. B. Konferenzräume und Equipment. Weitere Informationen finden Sie unter Arbeiten mit Ressourcen im WorkMail Amazon-Administratorhandbuch.	19. Oktober 2015
Support für das E-Mail-Migrationstool	Unterstützung für das E-Mail-Migrationstool. Weitere Informationen finden Sie unter Migration zu Amazon WorkMail im WorkMail Amazon-Administratorhandbuch.	16. August 2015
Vorschauversion von Amazon WorkMail	Die Vorschauversion von Amazon WorkMail.	28. Januar 2015

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.