aws

Guida per l'amministratore

Amazon WorkMail

Version 1.0

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

Amazon WorkMail: Guida per l'amministratore

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è Amazon WorkMail?

Amazon WorkMail è un servizio di posta elettronica e calendario aziendale sicuro e gestito con supporto per client di posta elettronica desktop e mobili esistenti. WorkMail Gli utenti di Amazon possono accedere alla propria posta elettronica, ai contatti e ai calendari utilizzando Microsoft Outlook, il proprio browser o le applicazioni di posta elettronica native per iOS e Android. Puoi integrare Amazon WorkMail con la tua directory aziendale esistente e controllare sia le chiavi che crittografano i tuoi dati sia la posizione in cui sono archiviati i tuoi dati.

Per un elenco degli endpoint e delle regioni AWS supportati, consulta Regioni geografiche ed endpoint AWS.

Argomenti

Requisiti WorkMail di sistema Amazon

Quando il tuo WorkMail amministratore Amazon ti invita ad accedere al tuo WorkMail account Amazon, puoi accedere utilizzando il client WorkMail web Amazon.

Amazon funziona WorkMail anche con tutti i principali dispositivi mobili e sistemi operativi che supportano il ActiveSync protocollo Exchange. Questi dispositivi includono iPad, iPhone, Android e Windows Phone. Gli utenti di macOS possono aggiungere il proprio WorkMail account Amazon alle app Mail, Calendar e Contatti.

Amazon WorkMail supporta le seguenti versioni del sistema operativo:

- Windows: Windows 7 SP1 o versione successiva
- macOS — macOS 10.12 (Sierra) o versione successiva
- Android: Andriod 5.0 o versioni successive
- iPhone — iOS 5 o versioni successive

- Windows phone: Windows 8.1 o versione successiva
- Blackberry — Sistema operativo Blackberry 10.3.3.3216

Se disponi di una licenza Microsoft Outlook valida, puoi accedere ad Amazon WorkMail utilizzando le seguenti versioni di Microsoft Outlook:

- Outlook 2013 o versioni successive
- Outlook 2013 Click-to-Run o versione successiva
- Outlook per Mac 2016 o versione successiva

Puoi accedere al client WorkMail web Amazon utilizzando le seguenti versioni di browser:

- Google Chrome — versione 22 o successiva
- Mozilla Firefox — versione 27 o successiva
- Safari — versione 7 o successiva
- Internet Explorer — Versione 11
- Microsoft Edge

Puoi anche usare Amazon WorkMail con il tuo client IMAP preferito.

WorkMail Concetti di Amazon

La terminologia e i concetti fondamentali per la comprensione e l'uso di Amazon WorkMail sono descritti di seguito.

Organizzazione

: Una configurazione tenant per Amazon WorkMail.

Alias

: Un nome univoco a livello globale per identificare l'organizzazione. L'alias viene utilizzato per accedere all'applicazione WorkMail web Amazon (https://*alias*.awsapps.com/mail).

Domain

: L'indirizzo web che segue il simbolo in un indirizzo e-mail. @ È possibile aggiungere un dominio che riceve i messaggi di posta e li fa recapitare nelle mailbox dell'organizzazione.

Test di dominio di posta

Durante la configurazione viene configurato automaticamente un dominio che può essere utilizzato per testare Amazon WorkMail. Il dominio di posta di prova è *alias* .awsapps.com e viene utilizzato come dominio predefinito se non configuri il tuo dominio. Il dominio di posta di test è soggetto a diversi limiti. Per ulteriori informazioni, consulta WorkMail Quote Amazon.

Directory

Un AWS Simple AD, AWS Managed AD o AD Connector creato in AWS Directory Service. Se crei un'organizzazione utilizzando la configurazione Amazon WorkMail Quick, creiamo una WorkMail directory per te. Non puoi visualizzare una WorkMail directory in AWS Directory Service.

Utente

Un utente creato in AWS Directory Service. L'utente può essere creato con un ruolo USER o REMOTE_USER. Quando un utente viene creato e abilitato con un ruolo USER, riceve la propria casella di posta a cui accedere. Quando un utente è disabilitato, non può accedere ad Amazon WorkMail.

L'utente creato e abilitato con un ruolo REMOTE_USER è elencato nella rubrica ma non ottiene una casella di posta in Amazon. WorkMail REMOTE_USER può avere la casella di posta ospitata all'esterno di Amazon, WorkMail ma sarà comunque elencato come qualsiasi altro utente con cassetta postale nella WorkMail rubrica di Amazon e potrà cercare nel calendario dell'altro utente per trovare informazioni su posti liberi o occupati.

Group (Gruppo)

Un gruppo utilizzato in. AWS Directory Service Un gruppo può essere utilizzato come lista di distribuzione o gruppo di sicurezza in Amazon WorkMail. I gruppi non dispongono di caselle di posta proprie.

Risorsa

Una risorsa rappresenta una sala riunioni o una risorsa attrezzatura che può essere prenotata dagli WorkMail utenti Amazon.

Policy per dispositivi mobili

Diverse regole di policy IT che controllano le caratteristiche e il comportamento di sicurezza di un dispositivo mobile.

Servizi AWS correlati

I seguenti servizi vengono utilizzati insieme ad Amazon WorkMail:

- AWS Directory Service—Puoi integrare Amazon WorkMail con un connettore AWS Simple AD, AWS Managed AD o AD Connector esistente. Crea una directory in AWS Directory Service e quindi abilita Amazon WorkMail per questa directory. Dopo aver configurato questa integrazione, puoi scegliere quali utenti abilitare per Amazon WorkMail da un elenco di utenti nella tua directory esistente e gli utenti possono accedere utilizzando le loro credenziali Active Directory esistenti. Per ulteriori informazioni, consulta la Guida AWS Directory Service all'amministrazione.
- Amazon Simple Email Service: Amazon WorkMail utilizza Amazon SES per inviare tutte le e-mail in uscita. Il dominio di posta di prova e i tuoi domini sono disponibili per la gestione nella console Amazon SES. Non è previsto alcun costo per le e-mail in uscita inviate da Amazon WorkMail. Per ulteriori informazioni, consulta la Amazon Simple Email Service Developer Guide.
- AWS Identity and Access Management AWS Management Console —Richiede il tuo nome utente e la tua password in modo che qualsiasi servizio che utilizzi possa determinare se sei autorizzato ad accedere alle sue risorse. Ti consigliamo di evitare di utilizzare le credenziali dell'account AWS per accedere AWS perché le credenziali AWS dell'account non possono essere revocate o limitate in alcun modo. Ti consigliamo invece di creare un utente IAM e aggiungerlo a un gruppo IAM con autorizzazioni amministrative. Puoi quindi accedere alla console utilizzando le credenziali utente IAM.

  Se hai effettuato la registrazione ad AWS senza creare un utente IAM, puoi crearne uno mediante la console IAM. Per ulteriori informazioni, consulta Creare singoli utenti IAM nella Guida per l'utente IAM.
- AWS Key Management Service—Amazon WorkMail è integrato AWS KMS per la crittografia dei dati dei clienti. La gestione delle chiavi può essere eseguita dalla AWS KMS console. Per ulteriori informazioni, consulta Cosa contiene la AWS Key Management Service Guida per gli AWS Key Management Service sviluppatori.

WorkMail Prezzi Amazon

Con Amazon WorkMail, non ci sono commissioni o impegni iniziali. I prezzi sono calcolati in base agli account utente attivi. Per informazioni specifiche sui prezzi, consultare l'articolo relativo ai prezzi.

WorkMail Risorse Amazon

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di questo servizio.

- Corsi e workshop: collegamenti a corsi specializzati e basati su ruoli, oltre a laboratori di autoapprendimento per aiutarti ad affinare le tue abilità e acquisire esperienza pratica. AWS
- AWS Developer Center: esplora i tutorial, scarica strumenti e scopri gli eventi per sviluppatori. AWS
- AWS Strumenti per sviluppatori: collegamenti a strumenti di sviluppo SDKs, toolkit IDE e strumenti da riga di comando per lo sviluppo e la gestione di applicazioni. AWS
- Centro risorse introduttivo: scopri come configurare Account AWS, entrare a far parte della AWS community e lanciare la tua prima applicazione.
- Tutorial pratici: segui i tutorial per avviare la step-by-step tua prima applicazione su. AWS
- AWS Whitepaper: collegamenti a un elenco completo di AWS white paper tecnici, su argomenti quali architettura, sicurezza ed economia e redatti da Solutions Architects o altri esperti tecnici. AWS
- Supporto AWS Center: l'hub per la creazione e la gestione dei casi. Supporto AWS Include anche collegamenti ad altre risorse utili, come forum, informazioni tecniche FAQs, stato di salute del servizio e AWS Trusted Advisor.
- Supporto— La pagina web principale per informazioni su Supporto one-on-one, un canale di supporto a risposta rapida per aiutarti a creare ed eseguire applicazioni nel cloud.
- Contatti - Un punto di contatto centrale per richieste relative a fatturazione, account, eventi, uso illecito e altre questioni relative ad AWS .
- AWS Termini del sito: informazioni dettagliate sul nostro copyright e marchio, sull'account, sulla licenza e sull'accesso al sito e altri argomenti.

Prerequisiti

Per agire come WorkMail amministratore Amazon, è necessario un account AWS. Se non è stata ancora effettuata la registrazione per AWS, completare le seguenti operazioni per iniziare a usare il servizio.

Argomenti

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Concedi le autorizzazioni agli utenti IAM per Amazon WorkMail

Per impostazione predefinita, gli utenti IAM non dispongono delle autorizzazioni per gestire le WorkMail risorse Amazon. Devi allegare una policy gestita da AWS (AmazonWorkMailFullAccesso AmazonWorkMailReadOnlyAccess) o creare una policy gestita dal cliente che conceda esplicitamente tali autorizzazioni agli utenti IAM. Quindi, colleghi questa policy agli utenti o ai gruppi IAM che hanno bisogno delle autorizzazioni. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per Amazon WorkMail.

Sicurezza in Amazon WorkMail

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per maggiori informazioni sui programmi di conformità applicabili ad Amazon WorkMail, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon WorkMail. I seguenti argomenti mostrano come configurare Amazon per WorkMail soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a usare altri servizi AWS che ti aiutano a monitorare e proteggere le tue WorkMail risorse Amazon.

Argomenti

Protezione dei dati in Amazon WorkMail

Il modello di responsabilità AWS condivisa Modello di si applica alla protezione dei dati in Amazon WorkMail. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon WorkMail o altri Servizi AWS utenti utilizzando la console, l'API o AWS SDKs. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Come WorkMail utilizza Amazon AWS KMS

Amazon crittografa in WorkMail modo trasparente tutti i messaggi nelle caselle di posta di tutte le WorkMail organizzazioni Amazon prima che i messaggi vengano scritti su disco e decrittografa in modo trasparente i messaggi quando gli utenti vi accedono. Non puoi disabilitare la crittografia. Per proteggere le chiavi di crittografia che proteggono i messaggi, Amazon WorkMail è integrato con AWS Key Management Service (AWS KMS).

Amazon offre WorkMail anche un'opzione per consentire agli utenti di inviare e-mail firmate o crittografate. Questa caratteristica di crittografia non utilizza AWS KMS. Per ulteriori informazioni, consulta Abilitazione di e-mail crittografate o firmate.

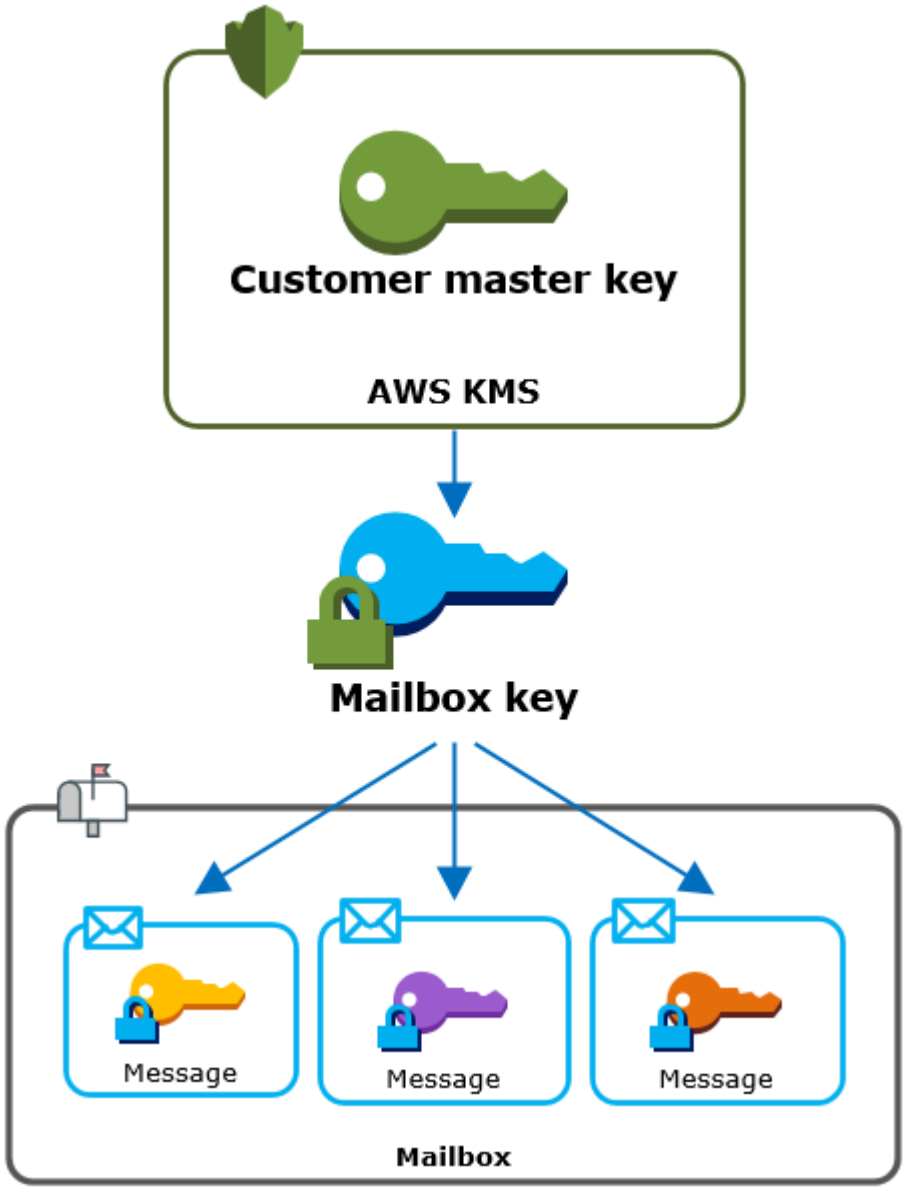
Argomenti

WorkMail Crittografia Amazon

In Amazon WorkMail, ogni organizzazione può contenere più caselle di posta, una per ogni utente dell'organizzazione. Tutti i messaggi, inclusi gli elementi di calendario ed e-mail, vengono archiviati nella casella di posta dell'utente.

Per proteggere il contenuto delle caselle di posta nelle tue WorkMail organizzazioni Amazon, Amazon WorkMail crittografa tutti i messaggi delle caselle di posta prima che vengano scritti su disco. Nessuna informazione fornita dai clienti viene archiviata in testo non crittografato.

Ogni messaggio viene crittografato con una chiave di crittografia dei dati univoca. La chiave del messaggio è protetta da una chiave della casella di posta, che è una chiave di crittografia univoca che viene utilizzata solo per quella casella. La chiave della casella di posta è crittografata con una chiave master AWS KMS del cliente (CMK) per l'organizzazione che non esce mai non crittografata. AWS KMS Il seguente diagramma mostra la relazione dei messaggi crittografati, le chiavi dei messaggi crittografati, la chiave della casella di posta crittografata e la CMK per l'organizzazione in AWS KMS.



Impostazione di un CMK per l'organizzazione

Quando crei un' WorkMail organizzazione Amazon, hai la possibilità di selezionare una chiave master AWS KMS del cliente (CMK) per l'organizzazione. Questa CMK protegge tutte le chiavi delle caselle di posta in quell'organizzazione.

Puoi selezionare la CMK AWS gestita predefinita per Amazon WorkMail oppure puoi selezionare una CMK gestita dal cliente esistente che possiedi e gestisci. Per ulteriori informazioni, consulta Customer Master Keys (CMKs) nella AWS Key Management Service Developer Guide. È possibile selezionare la stessa CMK o una CMK diversa per ciascuna organizzazione, ma non è possibile modificare la CMK dopo averla selezionata.

> **Important**
>
> Amazon WorkMail supporta solo sistemi simmetrici CMKs. Non puoi usare una CMK asimmetrica. Per informazioni su come determinare se una CMK è simmetrica o asimmetrica, consulta Identification symmetric and asimmetric nella Developer Guide. CMKs AWS Key Management Service

Per trovare la CMK adatta alla tua organizzazione, utilizza la voce di registro verso cui vengono registrate le chiamate. AWS CloudTrail AWS KMS

Una chiave di crittografia univoca per ogni casella di posta

Quando crei una casella di posta, Amazon WorkMail genera una chiave di crittografia simmetrica Advanced Encryption Standard (AES) unica a 256 bit per la casella di posta, nota come chiave della casella di posta, all'esterno di. AWS KMS Amazon WorkMail utilizza la chiave della casella di posta per proteggere le chiavi di crittografia per ogni messaggio nella casella di posta.

Per proteggere la chiave della casella di posta, Amazon WorkMail chiede di AWS KMS crittografare la chiave della casella di posta con il CMK dell'organizzazione. Quindi archivia la chiave della casella di posta crittografata nei metadati della casella.

> **Note**
>
> Amazon WorkMail utilizza una chiave di crittografia simmetrica delle caselle di posta per proteggere le chiavi dei messaggi. In precedenza, Amazon WorkMail proteggeva ogni casella di posta con una coppia di chiavi asimmetrica. Usava la chiave pubblica per crittografare ogni chiave di messaggio e la chiave privata per decrittografarla. La chiave della casella di posta privata era protetta dalla CMK per l'organizzazione. Le cassette postali più vecchie possono utilizzare una coppia di chiavi di posta asimmetrica. Questa modifica non influisce sulla sicurezza della casellla di posta o dei messaggi.

Crittografia di ogni messaggio

Quando un utente aggiunge un messaggio a una casella di posta, Amazon WorkMail genera una chiave di crittografia simmetrica AES a 256 bit unica per il messaggio esterno. AWS KMS Usa questa chiave del messaggio per crittografare il messaggio. Amazon WorkMail crittografa la chiave del

messaggio sotto la chiave della casella di posta e archivia la chiave del messaggio crittografato con il messaggio. Quindi, crittografa la chiave della casella di posta con la CMK per l'organizzazione.

Creazione di una nuova casella di posta

Quando Amazon WorkMail crea una casella di posta, utilizza il seguente processo per preparare la cassetta postale a contenere messaggi crittografati.

- Amazon WorkMail genera un'esclusiva chiave di crittografia simmetrica AES a 256 bit per la casella di posta esterna ad AWS KMS.
- Amazon WorkMail chiama l'operazione AWS KMS Encrypt. Passa la chiave della casella di posta e l'identificatore della chiave master del cliente (CMK) per l'organizzazione. AWS KMS restituisce un testo cifrato della chiave della casella di posta crittografata con CMK.
- Amazon WorkMail archivia la chiave crittografata della casella di posta con i metadati della casella di posta.

Crittografia di un messaggio di casella di posta

Per crittografare un messaggio, Amazon WorkMail utilizza il seguente processo.

1. Amazon WorkMail genera una chiave simmetrica AES unica a 256 bit per il messaggio. Utilizza la chiave del messaggio in testo semplice e l'algoritmo Advanced Encryption Standard (AES) per crittografare il messaggio all'esterno di. AWS KMS
2. Per proteggere la chiave del messaggio contenuta nella chiave della casella di posta, Amazon WorkMail deve decrittografare la chiave della casella di posta, che viene sempre archiviata in forma crittografata.

   Amazon WorkMail chiama l'operazione AWS KMS Decrypt e inserisce la chiave della casella di posta crittografata. AWS KMS utilizza la CMK per consentire all'organizzazione di decrittografare la chiave della casella di posta e restituisce la chiave della casella di posta in testo semplice ad Amazon. WorkMail
3. Amazon WorkMail utilizza la chiave della casella di posta in chiaro e l'algoritmo Advanced Encryption Standard (AES) per crittografare la chiave del messaggio all'esterno di. AWS KMS
4. Amazon WorkMail memorizza la chiave del messaggio crittografato nei metadati del messaggio crittografato in modo che sia disponibile per la decrittografia.

Decrittografia di un messaggio di casella di posta

Per decrittografare un messaggio, Amazon WorkMail utilizza il seguente processo.

1. Amazon WorkMail chiama l'operazione AWS KMS Decrypt e inserisce la chiave della casella di posta crittografata. AWS KMS utilizza la CMK per consentire all'organizzazione di decrittografare la chiave della casella di posta e restituisce la chiave della casella di posta in testo semplice ad Amazon. WorkMail
2. Amazon WorkMail utilizza la chiave della casella di posta in testo semplice e l'algoritmo Advanced Encryption Standard (AES) per decrittografare la chiave del messaggio crittografato all'esterno di. AWS KMS
3. Amazon WorkMail utilizza la chiave del messaggio in testo semplice per decrittografare il messaggio crittografato.

Memorizzazione delle chiavi delle caselle di posta

Per migliorare le prestazioni e ridurre al minimo le chiamate a AWS KMS, Amazon WorkMail memorizza nella cache ogni chiave della casella di posta in testo semplice per ogni client localmente per un massimo di un minuto. Al termine del periodo di memorizzazione, la chiave della casella di posta viene rimossa. Se la chiave della casella di posta per quel client è richiesta durante il periodo di memorizzazione nella cache, Amazon WorkMail può recuperarla dalla cache anziché chiamare. AWS KMS La chiave è protetta nella cache e non viene mai scritta su disco in testo non crittografato.

Autorizzazione dell'utilizzo di CMK

Quando Amazon WorkMail utilizza una chiave master del cliente (CMK) nelle operazioni crittografiche, agisce per conto dell'amministratore della casella di posta.

Per utilizzare la chiave master AWS KMS del cliente (CMK) come segreto per tuo conto, l'amministratore deve disporre delle seguenti autorizzazioni. È possibile specificare queste autorizzazioni necessarie in una policy IAM o delle chiavi.

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

Per consentire l'utilizzo della CMK solo per le richieste che provengono da Amazon WorkMail, puoi utilizzare la chiave kms: ViaService condition con il `workmail.<region>.amazonaws.com` valore.

Puoi inoltre utilizzare le chiavi o i valori nel contesto di crittografia come condizione per utilizzare la CMK per le operazioni di crittografia. Ad esempio, è possibile utilizzare un operatore di condizione stringa in un documento di policy IAM o delle chiavi oppure utilizzare un vincolo di concessione in una concessione.

Policy della chiave per la CMK gestita da AWS

La politica chiave per la CMK AWS gestita per Amazon WorkMail consente agli utenti di utilizzare la CMK per operazioni specifiche solo quando Amazon WorkMail effettua la richiesta per conto dell'utente. La policy delle chiavi non consente ad alcun utente di utilizzare la CMK direttamente.

Questa policy delle chiavi, come le policy di tutte le chiavi gestite da AWS, viene stabilita dal servizio. Non puoi modificare la politica chiave, ma puoi visualizzarla in qualsiasi momento. Per i dettagli, consulta Visualizzazione di una politica chiave nella Guida per gli AWS Key Management Service sviluppatori.

Le istruzioni di policy nella policy delle chiavi hanno l'effetto seguente:

- Consenti agli utenti dell'account e della regione di utilizzare la CMK per operazioni crittografiche e creare sovvenzioni, ma solo quando la richiesta proviene da Amazon per loro WorkMail conto. La chiave di condizione `kms:ViaService` applica questa limitazione.
- Consente all' AWS account di creare politiche IAM che consentono agli utenti di visualizzare le proprietà CMK e revocare le concessioni.

Di seguito è riportata una politica chiave per un esempio di CMK AWS gestito per 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" : "*"
  } ]
}
```

Utilizzo delle sovvenzioni per autorizzare Amazon WorkMail

Oltre alle politiche chiave, Amazon WorkMail utilizza le sovvenzioni per aggiungere autorizzazioni alla CMK per ogni organizzazione. Per visualizzare le sovvenzioni sulla CMK nel tuo account, utilizza l'operazione. ListGrants

Amazon WorkMail utilizza le sovvenzioni per aggiungere le seguenti autorizzazioni alla CMK per l'organizzazione.

- Aggiungi l'`kms:Encrypt`autorizzazione per consentire ad Amazon di WorkMail crittografare la chiave della casella di posta.
- Aggiungi l'`kms:Decrypt`autorizzazione per consentire ad Amazon di WorkMail utilizzare la CMK per decrittografare la chiave della casella di posta. Amazon WorkMail richiede questa autorizzazione in una concessione perché la richiesta di lettura dei messaggi della casella di posta utilizza il contesto di sicurezza dell'utente che sta leggendo il messaggio. La richiesta non utilizza le credenziali dell' AWS account. Amazon WorkMail crea questa sovvenzione quando selezioni una CMK per l'organizzazione.

Per creare le sovvenzioni, Amazon WorkMail chiama per CreateGrantconto dell'utente che ha creato l'organizzazione. L'autorizzazione a creare la concessione proviene dalla policy delle chiavi. Questa politica consente agli utenti dell'account di utilizzare la CMK dell'organizzazione quando Amazon WorkMail effettua la richiesta per conto di un utente autorizzato. `CreateGrant`

La policy chiave consente inoltre all'account root di revocare la concessione sulla chiave gestita AWS . Tuttavia, se revochi la concessione, Amazon non WorkMail può decrittografare i dati crittografati nelle tue caselle di posta.

Contesto WorkMail di crittografia Amazon

Un contesto di crittografia è un set di coppie chiave-valore che contiene dati arbitrari non segreti. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, associa AWS KMS crittograficamente il contesto di crittografia ai dati crittografati. lo stesso contesto di crittografia sia necessario per decrittografare i dati. Per ulteriori informazioni, consultare Contesto della crittografia nella Guida per gli sviluppatori di AWS Key Management Service .

Amazon WorkMail utilizza lo stesso formato di contesto di crittografia in tutte le operazioni AWS KMS crittografiche. È possibile utilizzare il contesto di crittografia per identificare un'operazione di crittografia in record e log di audit, ad esempio AWS CloudTrail, nonché come una condizione per l'autorizzazione in policy e concessioni.

Nelle sue richieste Encrypt and Decrypt a, AWS KMS Amazon WorkMail utilizza un contesto di crittografia in cui la chiave `aws:workmail:arn` e il valore è l'Amazon Resource Name (ARN) dell'organizzazione.

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

Ad esempio, il seguente contesto di crittografia include un esempio di ARN dell'organizzazione nella regione Europa (Irlanda) (`eu-west-1`).

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

Monitoraggio WorkMail dell'interazione di Amazon con AWS KMS

Puoi utilizzare AWS CloudTrail Amazon CloudWatch Logs per tenere traccia delle richieste a cui Amazon WorkMail invia per tuo AWS KMS conto.

Crittografa

Quando crei una casella di posta, Amazon WorkMail genera una chiave della casella di posta e chiama AWS KMS per crittografare la chiave della casella di posta. Amazon WorkMail invia una

richiesta Encrypt a AWS KMS con la chiave della casella di posta in testo semplice e un identificatore per la CMK dell'organizzazione Amazon. WorkMail

L'evento che registra l'operazione `Encrypt` è simile a quello del seguente evento di esempio. L'utente è il WorkMail servizio Amazon. I parametri includono l'ID CMK (`keyId`) e il contesto di crittografia per l' WorkMail organizzazione Amazon. Amazon WorkMail inserisce anche la chiave della casella di posta, ma questa non viene registrata nel CloudTrail registro.


```
{
    "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

Quando aggiungi, visualizzi o elimini un messaggio della casella di posta, Amazon WorkMail chiede di decrittografare la AWS KMS chiave della casella di posta. Amazon WorkMail invia una richiesta Decrypt a AWS KMS con la chiave della casella di posta crittografata e un identificatore per la CMK dell'organizzazione Amazon. WorkMail

L'evento che registra l'operazione `Decrypt` è simile a quello del seguente evento di esempio. L'utente è il WorkMail servizio Amazon. I parametri includono la chiave della casella di posta crittografata (come blob di testo cifrato), che non è registrata nel registro, e il contesto di crittografia per l'organizzazione Amazon. WorkMail AWS KMS ricava l'ID della CMK dal testo cifrato.

```
{
    "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"
}
```

Gestione delle identità e degli accessi per Amazon WorkMail

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon. WorkMail IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come WorkMail funziona Amazon con IAM
- Esempi di policy WorkMail basate sull'identità di Amazon
- Risoluzione dei problemi relativi all' WorkMail identità e all'accesso ad Amazon

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon WorkMail.

Utente del servizio: se utilizzi il WorkMail servizio Amazon per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più WorkMail funzionalità di Amazon per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon WorkMail, consultaRisoluzione dei problemi relativi all' WorkMail identità e all'accesso ad Amazon.

Amministratore del servizio: se sei responsabile delle WorkMail risorse Amazon della tua azienda, probabilmente hai pieno accesso ad Amazon WorkMail. È tuo compito determinare a quali WorkMail

funzionalità e risorse di Amazon devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon WorkMail, consultaCome WorkMail funziona Amazon con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso ad Amazon WorkMail. Per visualizzare esempi di policy WorkMail basate sull'identità di Amazon che puoi utilizzare in IAM, consulta. Esempi di policy WorkMail basate sull'identità di Amazon

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o

utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire

da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come WorkMail funziona Amazon con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon WorkMail, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con Amazon WorkMail. Per avere una visione di alto livello di come Amazon WorkMail e altri AWS servizi funzionano con IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Argomenti

- WorkMailPolitiche basate sull'identità di Amazon
- Politiche basate WorkMail sulle risorse di Amazon
- Autorizzazione basata sui WorkMail tag Amazon
- Ruoli Amazon WorkMail IAM

WorkMailPolitiche basate sull'identità di Amazon

Con le policy basate su identità di IAM, è possibile specificare quali azioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. Amazon WorkMail supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Operazioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione

AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche in Amazon WorkMail utilizzano il seguente prefisso prima dell'azione:`workmail:`. Ad esempio, per concedere a qualcuno l'autorizzazione a recuperare un elenco di utenti con il funzionamento dell' WorkMail `ListUsers`API Amazon, includi l'`workmail:ListUsers`azione nella sua politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Amazon WorkMail definisce il proprio set di azioni che descrivono le attività che puoi eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

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

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `List`, includi la seguente azione:

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

Per visualizzare un elenco di WorkMail azioni Amazon, consulta Actions defined by Amazon WorkMail nella IAM User Guide.

Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le operazioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Amazon WorkMail supporta le autorizzazioni a livello di risorsa per le organizzazioni Amazon. WorkMail

La risorsa WorkMail dell'organizzazione Amazon ha il seguente ARN:

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

Per ulteriori informazioni sul formato di ARNs, consulta Amazon Resource Names (ARNs) e AWS service namespaces.

Ad esempio, per specificare l'organizzazione `m-n1pq2345678r901st2u3vx45x6789yza` nell'istruzione, utilizza il seguente ARN:

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

Per specificare tutte le organizzazioni che appartengono a un account specifico, utilizza il carattere jolly (*):

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

Alcune WorkMail azioni di Amazon, come quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

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

Per visualizzare un elenco dei tipi di WorkMail risorse Amazon e relativi ARNs, consulta Resources defined by Amazon WorkMail nella IAM User Guide. Per sapere con quali azioni puoi specificare per l'ARN di ogni risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon. WorkMail

Chiavi di condizione

Amazon WorkMail supporta le seguenti chiavi di condizione globali.

- aws:CurrentTime
- aws:EpochTime
- aws:MultiFactorAuthAge
- aws:MultiFactorAuthPresent
- aws:PrincipalOrgID
- aws:PrincipalArn
- aws:RequestedRegion
- aws:SecureTransport
- aws:UserAgent

La seguente policy di esempio concede l'accesso alla WorkMail console Amazon solo dai principali IAM autenticati da MFA nella eu-west-1 regione AWS.

```
{
    "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
```

```
                }
            }
        }
    ]
}
```

Per visualizzare tutte le chiavi di condizione AWS globale, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

`workmail:ImpersonationRoleId`è l'unica chiave di condizione specifica del servizio supportata da Amazon. WorkMail

L'esempio seguente di policy riporta l'`AssumeImpersonationRole`azione a una particolare WorkMail organizzazione e ruolo di impersonificazione.

```
{
  "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"
        }
      }
    }
  ]
}
```

Esempi

Per visualizzare esempi di politiche WorkMail basate sull'identità di Amazon, consulta. Esempi di policy WorkMail basate sull'identità di Amazon

Politiche basate WorkMail sulle risorse di Amazon

Amazon WorkMail non supporta politiche basate sulle risorse.

Autorizzazione basata sui WorkMail tag Amazon

Puoi allegare tag alle WorkMail risorse Amazon o passare i tag in una richiesta ad Amazon WorkMail. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Per ulteriori informazioni sull'etichettatura WorkMail delle risorse Amazon, consultaTagging di un'organizzazione.

Ruoli Amazon WorkMail IAM

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Amazon WorkMail

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Puoi ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo. GetFederationToken

Amazon WorkMail supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Amazon WorkMail supporta ruoli collegati ai servizi. Per dettagli sulla creazione o la gestione di ruoli WorkMail collegati ad Amazon Service, consulta. Utilizzo di ruoli collegati ai servizi per Amazon WorkMail

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

Amazon WorkMail supporta i ruoli di servizio.

Esempi di policy WorkMail basate sull'identità di Amazon

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare WorkMail risorse Amazon. Inoltre, non possono eseguire attività utilizzando l' AWS API AWS Management Console AWS CLI, o. Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consultare Creazione di policy nella scheda JSON nella Guida per l'utente di IAM.

Argomenti

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare WorkMail risorse Amazon nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della WorkMail console Amazon

Per accedere alla WorkMail console Amazon, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle WorkMail risorse Amazon presenti nel tuo AWS account. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy.

Per garantire che tali entità possano ancora utilizzare la WorkMail console Amazon, allega anche la seguente politica AWS gestita alle entità. AmazonWorkMailFullAccess Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

La AmazonWorkMailFullAccesspolicy garantisce a un utente IAM l'accesso completo alle WorkMail risorse Amazon. Questa politica consente all'utente di accedere a tutte le operazioni e a tutte le AWS Directory Service operazioni di Amazon WorkMail AWS Key Management Service, Amazon Simple Email Service. Ciò include anche diverse EC2 operazioni Amazon che Amazon WorkMail

deve eseguire per tuo conto. Le `cloudwatch` autorizzazioni `logs` e sono necessarie per la registrazione degli eventi e-mail e la visualizzazione delle metriche nella console Amazon. WorkMail La registrazione di audit utilizza CloudWatch Logs, Amazon S3 e Amazon FireHose Data per l'archiviazione. `logs` Per ulteriori informazioni, consulta Registrazione e monitoraggio 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"
            }
        }
    }
  ]
}
```

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso o l' AWS CLI API. AWS Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Consenti agli utenti l'accesso in sola lettura alle risorse Amazon WorkMail

La seguente dichiarazione politica concede a un utente IAM l'accesso in sola lettura alle risorse Amazon. WorkMail Questa policy offre lo stesso livello di accesso della policy gestita da AWS AmazonWorkMailReadOnlyAccess. Entrambe le policy consentono all'utente di accedere a tutte le WorkMail `Describe` operazioni di Amazon. L'accesso all' AWS Directory Service `DescribeDirectories`operazione è necessario per ottenere informazioni sulle tue AWS Directory Service directory. L'accesso al servizio Amazon SES è necessario per ottenere informazioni sui domini configurati. L'accesso a AWS Key Management Service è necessario per ottenere informazioni sulle chiavi di crittografia utilizzate. Le `cloudwatch` autorizzazioni `logs` e sono necessarie per la registrazione degli eventi e-mail e la visualizzazione delle metriche nella console Amazon. WorkMail La registrazione di audit utilizza CloudWatch Logs, Amazon S3 e Amazon FireHose Data per l'archiviazione. `logs` Per ulteriori informazioni, consulta Registrazione e monitoraggio 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": "*"
    }
  ]
}
```

Risoluzione dei problemi relativi all' WorkMail identità e all'accesso ad Amazon

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon WorkMail e IAM.

Argomenti

Non sono autorizzato a eseguire un'azione in Amazon WorkMail

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

Il seguente errore di esempio si verifica quando l'utente `mateojackson` IAM tenta di utilizzare la console per visualizzare i dettagli su un gruppo ma non dispone `workmail:DescribeGroup` delle autorizzazioni.

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

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa `group` utilizzando l'azione `workmail:DescribeGroup`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon WorkMail.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon WorkMail. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie WorkMail risorse Amazon

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon WorkMail supporta queste funzionalità, consultaCome WorkMail funziona Amazon con IAM.

- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

AWS politiche gestite per Amazon WorkMail

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite che scrivere le politiche da soli. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AmazonWorkMailFullAccess

È possibile allegare la policy `AmazonWorkMailFullAccess` alle identità IAM. Questa politica concede autorizzazioni che consentono l'accesso completo ad Amazon. WorkMail

Per visualizzare le autorizzazioni per questa policy, consulta AmazonWorkMailFullAccess in AWS Management Console.

AWS politica gestita: AmazonWorkMailReadOnlyAccess

È possibile allegare la policy `AmazonWorkMailReadOnlyAccess` alle identità IAM. Questa politica concede autorizzazioni che consentono l'accesso in sola lettura ad Amazon. WorkMail

Per visualizzare le autorizzazioni per questa policy, consulta AmazonWorkMailReadOnlyAccess in AWS Management Console.

AWS politica gestita: AmazonWorkMailEventsServiceRolePolicy

Questa policy è associata al ruolo collegato ai servizi denominato AmazonWorkMailEventsper consentire l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da Amazon WorkMail Events. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon WorkMail.

WorkMail Aggiornamenti Amazon alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon WorkMail da quando questo servizio ha iniziato a tracciare queste modifiche.

Modifica	Descrizione	Data
Aggiornamenti delle policy gestite da AWS: aggiornamento a una policy esistente	Le `AmazonWorkMailFullAccess` autorizzazioni `AmazonWorkMailReadOnlyAccess` e sono state aggiornate per consentire WorkMail ad Amazon di supportare la registrazione di audit. Per ulteriori informazioni sulle autorizzazioni aggiornate, consulta Esempi di policy	14 febbraio 2024

Modifica	Descrizione	Data
	WorkMail basate sull'identità di Amazon e per informazioni sulla registrazione di controllo , consulta. Abilitazione della registrazione di controllo	
Amazon WorkMail ha iniziato a tracciare le modifiche	Amazon WorkMail ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	1 marzo 2021

Utilizzo di ruoli collegati ai servizi per Amazon WorkMail

Amazon WorkMail utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Amazon. WorkMail I ruoli collegati ai servizi sono predefiniti da Amazon WorkMail e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Un ruolo collegato al servizio semplifica la configurazione di Amazon WorkMail perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Amazon WorkMail definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Amazon WorkMail può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo avere eliminato le risorse correlate. In questo modo proteggi le tue WorkMail risorse Amazon perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione relativa ai servizi AWS che funzionano con IAM e cerca i servizi che nella colonna Service-Linked Role (Ruolo associato ai servizi) riportano Yes (Sì). Scegli un Sì con un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Amazon WorkMail

Amazon WorkMail utilizza il ruolo collegato ai servizi denominato: AmazonWorkMailEventsAmazon WorkMail utilizza questo ruolo collegato ai servizi per consentire l'accesso ai AWS servizi e alle

risorse utilizzati o gestiti dagli WorkMail eventi Amazon, come il monitoraggio degli eventi e-mail registrati da. CloudWatch Per ulteriori informazioni sull'attivazione della registrazione degli eventi e-mail per Amazon WorkMail, consultaAbilitazione della registrazione degli eventi via e-mail.

Il ruolo AmazonWorkMailEvents collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `events.workmail.amazonaws.com`

La politica di autorizzazione dei ruoli consente WorkMail ad Amazon di completare le seguenti azioni sulle risorse specificate:

- Operazione: `logs:CreateLogGroup` su `all AWS resources`
- Operazione: `logs:CreateLogStream` su `all AWS resources`
- Operazione: `logs:PutLogEvents` su `all AWS resources`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Amazon WorkMail

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando attivi la registrazione WorkMail degli eventi di Amazon e utilizzi le impostazioni predefinite nella WorkMail console Amazon, Amazon WorkMail crea il ruolo collegato ai servizi per te.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando attivi la registrazione WorkMail degli eventi di Amazon e utilizzi le impostazioni predefinite, Amazon WorkMail crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per Amazon WorkMail

Amazon WorkMail non ti consente di modificare il ruolo AmazonWorkMailEvents collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Amazon WorkMail

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il WorkMail servizio Amazon utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare WorkMail le risorse Amazon utilizzate da AmazonWorkMailEvents

1. Disattiva la registrazione WorkMail degli eventi di Amazon.
    a. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

       Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
    b. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
    c. Nel riquadro di navigazione, scegli Impostazioni dell'organizzazione, quindi scegli Monitoraggio.
    d. Per Log settings (Impostazioni di log), scegliere Edit (Modifica).
    e. Sposta il cursore Abilita eventi di posta elettronica in posizione OFF.
    f. Seleziona Salva.
2. Elimina il gruppo di CloudWatch log Amazon.
    a. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
    b. Scegliere Logs (Log).
    c. Per Log Groups (Gruppi di log), seleziona il gruppo di log da eliminare.
    d. Per Actions (Operazioni), scegli Delete log group (Elimina gruppo di log).

e. Scegliere Yes, Delete (Sì, elimina).

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AmazonWorkMailEvents collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati WorkMail ai servizi Amazon

Amazon WorkMail supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Amazon WorkMail Regions and Endpoints.

Registrazione e monitoraggio in Amazon WorkMail

Il monitoraggio e il controllo delle e-mail e dei log sono importanti per mantenere la salute della tua organizzazione Amazon WorkMail . Amazon WorkMail supporta due tipi di monitoraggio:

- Registrazione degli eventi: il monitoraggio dell'attività di invio di e-mail per la tua organizzazione aiuta a proteggere la reputazione del dominio. Il monitoraggio consente, inoltre, di tenere traccia delle e-mail inviate e ricevute. Per ulteriori informazioni su come abilitare la registrazione degli eventi e-mail, consulta Abilitazione della registrazione degli eventi via e-mail.
- Registrazione di audit: puoi utilizzare i log di controllo per acquisire informazioni dettagliate sull'utilizzo della tua WorkMail organizzazione Amazon, ad esempio monitorare l'accesso degli utenti alle caselle di posta, verificare eventuali attività sospette ed eseguire il debug del controllo degli accessi e delle configurazioni dei provider di disponibilità. Per ulteriori informazioni, consulta Abilitazione della registrazione di controllo.

AWS fornisce i seguenti strumenti di monitoraggio per monitorare Amazon WorkMail, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Ad esempio, quando abiliti la registrazione degli eventi e-mail per Amazon WorkMail, CloudWatch puoi tenere traccia delle e-mail inviate e ricevute per la tua organizzazione. Per ulteriori informazioni sul monitoraggio di Amazon WorkMail con CloudWatch, consultaMonitoraggio di Amazon WorkMail con CloudWatch metriche. Per ulteriori informazioni CloudWatch, consulta la Amazon CloudWatch User Guide.

- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi eventi e-mail e ai log di controllo per Amazon WorkMail quando la registrazione di e-mail e audit è abilitata nella console Amazon. WorkMail CloudWatch I log possono monitorare le informazioni nei file di registro e puoi archiviare i dati di registro in uno storage altamente durevole. Per ulteriori informazioni sul tracciamento dei WorkMail messaggi Amazon tramite CloudWatch Logs, consulta Abilitazione della registrazione degli eventi via e-mail eAbilitazione della registrazione di controllo. Per ulteriori informazioni sui CloudWatch log, consulta la Amazon CloudWatch Logs User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto tuo Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta Registrazione delle chiamate WorkMail API Amazon con AWS CloudTrail.
- Amazon S3 ti consente di archiviare e accedere ai tuoi WorkMail eventi Amazon in modo conveniente. Amazon S3 fornisce meccanismi per la gestione del ciclo di vita dei dati degli eventi, che consentono di configurare l'eliminazione automatica di vecchi eventi o configurare l'archiviazione automatica su Amazon S3 Glacier. Nota, la consegna Amazon S3 è disponibile solo per gli eventi di registrazione degli audit. Per ulteriori informazioni su Amazon S3, consulta la Amazon S3 User Guide.
- Amazon Data Firehose ti consente di trasmettere i dati dei tuoi eventi ad altri servizi AWS come Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Service, Amazon Serverless OpenSearch , Splunk e qualsiasi endpoint HTTP personalizzato o endpoint HTTP di proprietà di fornitori di servizi terzi supportati, tra cui Datadog LogicMonitor, Dynatrace, MongoDB, New Redshift Lic, Coralogix ed Elastic. OpenSearch La consegna a Firehose è disponibile solo per gli eventi di registrazione degli audit. Per ulteriori informazioni su Firehose, consulta la guida per sviluppatori di Amazon Data Firehose.

Argomenti

Monitoraggio di Amazon WorkMail con CloudWatch metriche

Puoi monitorare WorkMail l'utilizzo di Amazon CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili quasi in tempo reale. Le metriche gratuite vengono archiviate per 15 mesi in modo da poter accedere alle informazioni storiche per vedere le prestazioni della tua applicazione o del tuo servizio web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

CloudWatch metriche per Amazon WorkMail

Amazon WorkMail invia le seguenti metriche e informazioni sulle dimensioni a CloudWatch.

Lo spazio dei nomi `AWS/WorkMail` include le metriche descritte di seguito.

Metrica	Descrizione
`OrganizationEmailReceived`	Il numero di e-mail ricevute dalla tua WorkMail organizzazione Amazon. Se un'e-mail è indirizzata a 10 destinatari della tua organizza zione, il `OrganizationEmailReceived` conteggio è uno. Unità: numero
`MailboxEmailDelivered`	Il numero di e-mail recapitate alle singole caselle di posta della tua WorkMail organizza zione Amazon. Se un'e-mail viene recapitat a con successo a 10 destinatari della tua organizzazione, il `MailboxEmailDelive red` conteggio è 10. Unità: numero
`IncomingEmailBounced`	Il numero di e-mail in arrivo che sono state respinte a causa dell'esaurimento delle caselle di posta. Questo parametro viene conteggiato per ogni destinatario previsto. Ad esempio, se un'e-mail viene inviata a 10

Metrica	Descrizione
	destinatari dell'organizzazione e due destinatari dispongono di cassette postali piene, con conseguente risposta respinta, il conteggio è due. `IncomingEmailBounced` Unità: numero
`OutgoingEmailBounced`	Il numero di e-mail in uscita che non è stato possibile recapitare. Questo parametro viene conteggiato per ogni destinatario previsto. Ad esempio, se un'e-mail viene inviata a 10 destinatari e non è possibile recapitare due e-mail, il `OutgoingEmailBounced` conteggio è 2. Unità: numero
`OutgoingEmailSent`	Il numero di e-mail inviate con successo dalla tua WorkMail organizzazione Amazon. Questo parametro viene conteggiato per ogni destinatario di un'e-mail inviata correttamente. Ad esempio, se 1 e-mail viene inviata a 10 destinatari e l'e-mail è stata recapitata a 8 di essi, il conteggio `OutgoingEmailSent` è pari a 8. Unità: numero

Metrica	Descrizione
`AuthenticationFailure`	Questa metrica conta il numero di tentativi di autenticazione. Quando l'autenticazione ha esito positivo, il conteggio è 0 e quando l'autenticazione non ha esito positivo, il conteggio è 1. Utilizza la `Sum` statistica per monitorare il numero di tentativi di autenticazione falliti. Usa la `Sample count` statistica per monitorare il numero totale di eventi di autenticazione. Utilizza la `Average` statistica per monitorare il rapporto tra gli eventi di autenticazione falliti e quelli di autenticazione riusciti. Unità: numero
`AccessDenied`	Questa metrica conta il numero di valutazioni del controllo degli accessi. Quando l'azione viene negata dal controllo degli accessi, il conteggio è 1 e quando l'azione viene concessa, il conteggio è 0. Utilizza la `Sum` statistica per monitorare il volume delle azioni negate, la `Sample count` statistica per monitorare il numero totale di azioni tentate e la `Average` statistica per monitorare il rapporto tra azioni consentite e rifiutate. Unità: numero

Metrica	Descrizione
`ActionDenied`	Questa metrica viene conteggiata quando viene eseguita un'azione sui dati delle cassette postali. Quando l'azione viene negata, il conteggio è 1 e se l'azione viene concessa, il conteggio è 0. Utilizza la `Sum` statistica per monitorare il volume di azioni negate nella cassetta postale, la `Sample count` statistic a per monitorare il numero totale di tentativi di azioni sulla cassetta postale e la `Average` statistica per monitorare il rapporto tra azioni consentite e rifiutate. Unità: numero
`AvailabilityProviderFailure`	Questa metrica viene conteggiata per ogni richiesta del provider di disponibilità che Amazon WorkMail esegue per recuperare la disponibilità del calendario da una fonte esterna. Per ulteriori informazioni sugli Availabil ity Provider, consulta l'Amazon WorkMail Administrator Guide.

Monitoraggio dei registri degli eventi WorkMail e-mail di Amazon

Quando attivi la registrazione degli eventi e-mail per la tua WorkMail organizzazione Amazon, Amazon WorkMail registra gli eventi e-mail con. CloudWatch Per ulteriori informazioni sull'abilitazione della registrazione di eventi e-mail, consulta Abilitazione della registrazione degli eventi via e-mail.

Le tabelle seguenti descrivono gli eventi con cui Amazon WorkMail registra CloudWatch, quando vengono trasmessi e cosa contengono i campi degli eventi.

`ORGANIZATION_EMAIL_RECEIVED`

Questo evento viene registrato quando la tua WorkMail organizzazione Amazon riceve un messaggio e-mail.

Campo	Descrizione
recipients	I destinatari previsti del messaggio.
mittente	L'indirizzo e-mail dell'utente che ha inviato il messaggio e-mail per conto di un altro utente. Questo campo è impostato solo quando un'e-mail viene inviata per conto di un altro utente.
from	L'indirizzo Da, che di solito è l'indirizzo e-mail dell'utente che ha inviato il messaggio. Se l'utente ha inviato il messaggio come un altro utente o per conto di un altro utente, questo campo restituisce l'indirizzo e-mail per conto del quale è stata inviata l'e-mail e non l'indirizzo e-mail del mittente effettivo.
subject	Oggetto del messaggio e-mail.
messageId	ID messaggio SMTP.
spamVerdict	Indica se il messaggio è contrassegnato come spam da Amazon SES. Per ulteriori informazioni, consulta il contenuto delle notifiche per la ricezione di e-mail di Amazon SES nella Amazon Simple Email Service Developer Guide.
dkimVerdict	Indica se il controllo DomainKeys Identified Mail (DKIM) è stato superato. Per ulteriori informazioni, consulta il contenuto delle notifiche per la ricezione di e-mail di Amazon SES nella Amazon Simple Email Service Developer Guide.
dmarcVerdict	Indica se il controllo DMARC (Domain-based Message Authentication, Reporting and Conformance) è stato superato. Per

Campo	Descrizione
	ulteriori informazioni, consulta il contenuto delle notifiche per la ricezione di e-mail di Amazon SES nella Amazon Simple Email Service Developer Guide.
dmarcPolicy	Viene visualizzato solo quando il campo dmarcVerdict contiene "FAIL". Indica l'azione da eseguire sul messaggio di posta elettronica quando il controllo DMARC non riesce (NONE, QUARANTINE o REJECT). Questo comportamento è impostato dal proprietario del dominio di posta elettronica mittente.
spfVerdict	Indica se i controlli Sender Policy Framework (SPF) sono stati superati. Per ulteriori informazioni, consulta il contenuto delle notifiche per la ricezione di e-mail di Amazon SES nella Amazon Simple Email Service Developer Guide.
messageTimestamp	Indica quando il messaggio viene ricevuto.

`MAILBOX_EMAIL_DELIVERED`

Questo evento viene registrato quando un messaggio viene recapitato a una casella di posta nell'organizzazione. Viene registrato una volta per ogni casella di posta in cui un messaggio viene recapitato, pertanto un singolo evento `ORGANIZATION_EMAIL_RECEIVED` può risultare in più eventi `MAILBOX_EMAIL_DELIVERED`.

Campo	Descrizione
recipient	La casella di posta in cui il messaggio viene recapitato.
folder	La cartella della casella di posta in cui il messaggio viene collocato.

RULE_APPLIED

Questo evento viene registrato quando un messaggio in entrata o in uscita avvia una regola del flusso di posta elettronica.

Campo	Descrizione
ruleName	Nome della regola .
ruleType	Il tipo di regola applicata (INBOUND_RULE, OUTBOUND_RULE o MAILBOX_RULE). Le regole in entrata e in uscita si applicano alla tua organizzazione Amazon WorkMail. Le regole della casella di posta si applicano solo a caselle di posta specifiche. Per ulteriori informazioni, consulta Gestione dei flussi di e-mail.
ruleActions	Operazioni effettuate in base alla regola. Destinatari diversi del messaggio possono avere operazioni diverse, ad esempio un'e-mail non recapitata o un'e-mail recapitata.
targetFolder	Cartella di destinazione prevista per `Move` o `Copy` MAILBOX_RULE.
targetRecipient	Destinatario previsto di `Forward` o `Redirect` MAILBOX_RULE.

JOURNALING_INITIATED

Questo evento viene registrato quando Amazon WorkMail invia un'e-mail all'indirizzo di journaling specificato dall'amministratore dell'organizzazione. Questa viene trasmessa solo se l'indirizzo di journaling è configurato per l'organizzazione. Per ulteriori informazioni, consulta Usare l'e-mail journaling con Amazon WorkMail.

Campo	Descrizione
journalingAddress	L'indirizzo e-mail a cui viene inviato il messaggio di journaling.

INCOMING_EMAIL_BOUNCED

Questo evento viene registrato quando un messaggio in arrivo non può essere recapitato a un destinatario di destinazione. I messaggi di posta elettronica possono essere respinti per diversi motivi, ad esempio per una cassetta postale di destinazione completa. Il sistema registra questo evento una volta per ogni destinatario e il messaggio viene respinto. Ad esempio, se un messaggio in arrivo è indirizzato a tre destinatari e due di loro hanno caselle di posta piene, vengono registrati due eventi INCOMING_EMAIL_BOUNCED.

Campo	Descrizione
bouncedRecipient	Il destinatario previsto per il quale Amazon WorkMail ha inviato il messaggio.

OUTGOING_EMAIL_SUBMITTED

Questo evento viene registrato quando un utente nell'organizzazione invia un messaggio e-mail per l'invio. Questo viene registrato prima che il messaggio lasci Amazon WorkMail, quindi questo evento non indica se l'e-mail è stata recapitata correttamente.

Campo	Descrizione
recipients	I destinatari del messaggio come specificato dal mittente. Include tutti i destinatari sulla riga A, CC e CCN.
mittente	L'indirizzo e-mail dell'utente che ha inviato il messaggio e-mail per conto di un altro utente. Questo campo è impostato solo quando un'e-mail viene inviata per conto di un altro utente.

Campo	Descrizione
from	L'indirizzo Da, che di solito è l'indirizzo e-mail dell'utente che ha inviato il messaggio. Se l'utente ha inviato il messaggio come un altro utente o per conto di un altro utente, questo campo restituisce l'indirizzo e-mail per conto del quale è stata inviata l'e-mail e non l'indirizzo e-mail del mittente effettivo.
subject	Oggetto del messaggio e-mail.

`OUTGOING_EMAIL_SENT`

Questo evento viene registrato quando un'e-mail in uscita viene recapitata a un destinatario target. Questo viene registrato una volta per ogni destinatario che ha avuto esito positivo, pertanto una singola voce `OUTGOING_EMAIL_SUBMITTED` può risultate in più voci `OUTGOING_EMAIL_SENT`.

Campo	Descrizione
recipient	Il destinatario dell'e-mail recapitata.
mittente	L'indirizzo e-mail dell'utente che ha inviato il messaggio e-mail per conto di un altro utente. Questo campo è impostato solo quando un'e-mail viene inviata per conto di un altro utente.
from	L'indirizzo Da, che di solito è l'indirizzo e-mail dell'utente che ha inviato il messaggio. Se l'utente ha inviato il messaggio come un altro utente o per conto di un altro utente, questo campo restituisce l'indirizzo e-mail per conto del quale è stata inviata l'e-mail e non l'indirizzo e-mail del mittente effettivo.
messageId	ID messaggio SMTP.

OUTGOING_EMAIL_BOUNCED

Questo evento viene registrato quando un messaggio in uscita non può essere recapitato a un destinatario di destinazione. I messaggi di posta elettronica possono essere respinti per diversi motivi, ad esempio per una cassetta postale di destinazione completa. Il sistema registra un messaggio di mancato invio per ogni destinatario che genera un messaggio di posta elettronica respinto. Ad esempio, se un messaggio in uscita è indirizzato a tre destinatari e due di loro hanno caselle di posta piene, vengono registrati due eventi `OUTGOING_EMAIL_BOUNCED`.

Campo	Descrizione
bouncedRecipient	Il destinatario previsto per il quale il server di posta di destinazione non ha recapitato il messaggio.

DMARC_POLICY_APPLIED

Questo evento viene registrato quando una policy DMARC viene applicata a un messaggio di posta elettronica inviato all'organizzazione.

Campo	Descrizione
from	L'indirizzo Da, che di solito è l'indirizzo e-mail dell'utente che ha inviato il messaggio. Se l'utente ha inviato il messaggio come un altro utente o per conto di un altro utente, questo campo restituisce l'indirizzo e-mail per conto del quale è stata inviata l'e-mail e non l'indirizzo e-mail del mittente effettivo.
recipients	I destinatari previsti del messaggio.
policy	La policy DMARC applicata, che indica l'azione da intraprendere sul messaggio di posta elettronica quando il controllo DMARC non riesce (NONE, QUARANTINE o REJECT). Questo comportamento è uguale a quello del

Campo	Descrizione
	campo dmarcPolicy nell'evento ORGANIZATION_EMAIL_RECEIVED.

Monitoraggio dei log WorkMail di controllo di Amazon

Puoi utilizzare i log di controllo per monitorare l'accesso alle caselle di posta della tua Amazon WorkMail Organization. Amazon WorkMail registra cinque tipi di eventi di controllo e questi eventi possono essere pubblicati su CloudWatch Logs, Amazon S3 o Amazon Firehouse. Puoi utilizzare i log di controllo per monitorare l'interazione degli utenti con le caselle di posta dell'organizzazione, i tentativi di autenticazione, la valutazione delle regole di controllo degli accessi ed eseguire chiamate dei provider di disponibilità a sistemi esterni e monitorare gli eventi con token di accesso personali. Per informazioni sulla configurazione della registrazione di controllo, vedere. Abilitazione della registrazione di controllo

Le seguenti sezioni descrivono gli eventi di controllo registrati da Amazon WorkMail, quando gli eventi vengono trasmessi e le informazioni sui campi degli eventi.

Registri di accesso alle cassette postali

Gli eventi di accesso alla cassetta postale forniscono informazioni su quale azione è stata intrapresa (o tentata) su quale oggetto della cassetta postale. Viene generato un evento di accesso alla cassetta postale per ogni operazione che si tenta di eseguire su un elemento o una cartella in una cassetta postale. Questi eventi sono utili per controllare l'accesso ai dati delle cassette postali.

Campo	Descrizione
event_timestamp	Quando si è verificato l'evento, in millisecondi dall'epoca di Unix.
request_id	L'ID che identifica in modo univoco la richiesta.
organization_arn	L'ARN dell' WorkMail organizzazione & Amazon a cui appartiene l'utente autenticato.
user_id	L'ID dell'utente autenticato.

Campo	Descrizione
impersonator_id	L'ID dell'imitatore. Presente solo se la funzione di impersonificazione è stata utilizzata per la richiesta.
protocol	Il protocollo utilizzato. Il protocollo può essere: `AutoDiscover EWS`,`IMAP`,`WindowsOutlook` ,`ActiveSync` , `SMTPWebMail`,`IncomingEmail` , `oOutgoingEmail` .
source_ip	L'indirizzo IP di origine della richiesta.
user_agent	L'agente utente che ha effettuato la richiesta.
action	L'azione intrapresa sull'oggetto, che può essere: `readread_hierarchy` ,`read_summary` ,`read_attachment` ,`read_permissions` ,`create`,`update`,`update_permissions` , `update_read_state delete`,`submit_email_for_sending` ,`abort_sending_email` ,`move`,`move_to`,`copy`, `ocopy_to`.
owner_id	L'ID dell'utente proprietario dell'oggetto su cui si sta agendo.
object_type	Il tipo di oggetto, che può essere: cartella, messaggio o allegato.
id_articolo	L'ID che identifica in modo univoco il messaggio che è l'oggetto dell'evento o che contiene l'allegato che è l'oggetto dell'evento.
folder_path	Il percorso della cartella su cui si sta agendo o il percorso della cartella contenente l'elemento su cui si sta agendo.

Campo	Descrizione
folder_id	L'ID che identifica in modo univoco la cartella oggetto dell'evento o che contiene l'oggetto dell'evento.
pathment_path	Il percorso dei nomi visualizzati dell'allegato interessato.
action_allowed	Se l'azione è stata consentita. Può essere vero o falso.

Registri di controllo degli accessi

Gli eventi di controllo degli accessi vengono generati ogni volta che viene valutata una regola di controllo degli accessi. Questi registri sono utili per controllare gli accessi vietati o per eseguire il debug delle configurazioni di controllo degli accessi.

Campo	Descrizione
event_timestamp	Quando si è verificato l'evento, in millisecondi dall'epoca di Unix.
request_id	L'ID che identifica in modo univoco la richiesta.
organization_arn	L'ARN dell' WorkMail organizzazione a cui appartiene l'utente autenticato.
user_id	L'ID dell'utente autenticato.
impersonator_id	L'ID dell'imitatore. Presente solo se la funzione di impersonificazione è stata utilizzata per la richiesta.
protocol	Il protocollo utilizzato, che può essere:`AutoDiscover` ,,`EWS`,`IMAP`,`WindowsOutlook` ,`ActiveSync` , `SMTP`

Campo	Descrizione
	`WebMailIncomingEmail` , o. `OutgoingEmail`
source_ip	L'indirizzo IP di origine della richiesta.
scope	L'ambito della regola, che può essere:`AccessControl` , `DeviceAccessControl` o. `ImpersonationAccessControl`
rule_id	L'ID della regola di controllo degli accessi corrispondente. Quando non ci sono regole corrispondenti, rule_id non è disponibile.
access_granted	Se l'accesso era consentito. Può essere vero o falso.

Registri di autenticazione

Gli eventi di autenticazione contengono informazioni sui tentativi di autenticazione.

> **Note**
>
> Gli eventi di autenticazione non vengono generati per gli eventi di autenticazione tramite l' WorkMail WebMail applicazione Amazon.

Campo	Descrizione
event_timestamp	Quando si è verificato l'evento, in millisecondi dall'epoca Unix.
request_id	L'ID che identifica in modo univoco la richiesta.
organization_arn	L'ARN dell' WorkMail organizzazione a cui appartiene l'utente autenticato.

Campo	Descrizione
user_id	L'ID dell'utente autenticato.
Utente	Il nome utente con cui è stata tentata l'autenti cazione.
protocol	Il protocollo utilizzato, che può essere:`AutoDisco ver` ,`EWS`,`IMAP`,`WindowsOu tlook` ,`ActiveSync` ,`SMTP`, `WebMailIncomingEmail` , `oOutgoingE mail` .
source_ip	L'indirizzo IP di origine della richiesta.
user_agent	L'agente utente che ha effettuato la richiesta.
metodo	Il metodo di autenticazione. Attualmente è supportata solo la versione di base.
auth_successful	Se il tentativo di autenticazione ha avuto successo. Può essere vero o falso.
auth_failed_reason	Il motivo dell'errore di autenticazione. Presente solo se l'autenticazione non è riuscita.
personal_access_token_id	L'ID del token di accesso personale utilizzato per l'autenticazione.

Registri dei token di accesso personali

Un evento PAT (personal access token) viene generato per ogni tentativo di creare o eliminare un token di accesso personale. Gli eventi relativi ai token di accesso personali forniscono informazioni sulla corretta creazione dei token di accesso personali da parte degli utenti. I log dei token di accesso personali sono utili per controllare gli utenti finali che creano ed eliminano i propri. PATs L'accesso utente con token di accesso personali genererà eventi nei registri di autenticazione esistenti. Per ulteriori informazioni, consulta Registri di autenticazione.

Campo	Descrizione
event_timestamp	Quando si è verificato l'evento, in millisecondi dall'epoca Unix.
request_id	L'ID che identifica in modo univoco la richiesta.
organization_arn	L'ARN dell' WorkMail organizzazione a cui appartiene l'utente autenticato.
user_id	L'ID dell'utente autenticato.
Utente	Il nome utente dell'utente che ha eseguito questa azione.
protocol	È stato eseguito il protocollo utilizzato durante l'azione, che può essere: webapp
source_ip	L'indirizzo IP di origine della richiesta.
user_agent	L'agente utente che ha effettuato la richiesta.
action	L'azione del token di accesso personale, che può essere: creare o eliminare.
nome	Il nome del token di accesso personale.
expires_time	La data di scadenza del token di accesso personale.
ambiti	Gli ambiti delle autorizzazioni del token di accesso personale sulla casella di posta.

Registri dei provider di disponibilità

Gli eventi del provider di disponibilità vengono generati per ogni richiesta di disponibilità WorkMail che Amazon effettua per tuo conto al provider di disponibilità configurato. Questi eventi sono utili per eseguire il debug della configurazione del provider di disponibilità.

Campo	Descrizione
event_timestamp	Quando si è verificato l'evento, in millisecondi dall'epoca Unix.
request_id	L'ID che identifica in modo univoco la richiesta.
organization_arn	L'ARN dell' WorkMail organizzazione a cui appartiene l'utente autenticato.
user_id	L'ID dell'utente autenticato.
tipo	Il tipo di provider di disponibilità richiamato, che può essere: `EWS` o. `LAMBDA`
domain	Il dominio per il quale viene ottenuta la disponibilità.
function_arn	L'ARN della Lambda richiamata, se il tipo è LAMBDA. Altrimenti, questo campo non è presente.
ews_endpoint	Il tipo di endpoint EWS è EWS. Altrimenti, questo campo non è presente.
error_message	Il messaggio che descrive la causa dell'erro re. Se la richiesta è andata a buon fine, questo campo non è presente.
availability_event_successful	Se la richiesta di disponibilità è stata soddisfat ta con successo.

Utilizzo di CloudWatch Insights con Amazon WorkMail

Se hai attivato la registrazione degli eventi via e-mail nella WorkMail console Amazon o hai abilitato la consegna dei log di controllo a CloudWatch Logs, puoi utilizzare Amazon CloudWatch Logs Insights per interrogare i log degli eventi. Per ulteriori informazioni sull'abilitazione della registrazione di eventi e-mail, consulta Abilitazione della registrazione degli eventi via e-mail. Per ulteriori informazioni

su CloudWatch Logs Insights, consulta Analizza i dati di log con CloudWatch Logs Insights nella Amazon CloudWatch Logs User Guide.

Gli esempi seguenti mostrano come interrogare i CloudWatch log per eventi e-mail comuni. Queste interrogazioni vengono eseguite nella CloudWatch console. Per istruzioni su come eseguire queste query, consulta Tutorial: Esegui e modifica una query di esempio nella Amazon CloudWatch Logs User Guide.

Example Scopri perché l'utente B non ha ricevuto un'e-mail inviata dall'utente A.

Il seguente codice di esempio illustra come eseguire query su un'e-mail in uscita inviata da Utente A a Utente B, ordinata in base al timestamp.

```
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/)
```

Questo codice restituisce il messaggio inviato e l'ID di tracciamento. Utilizza l'ID di tracciamento nel codice di esempio seguente per eseguire query sui log di eventi per il messaggio inviato.

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

Questo codice restituisce l'ID messaggio e-mail e gli eventi e-mail. `OUTGOING_EMAIL_SENT` indica che l'e-mail è stata inviata. `OUTGOING_EMAIL_BOUNCED` indica che l'e-mail non è stata recapitata. Per vedere se l'e-mail è stata ricevuta, esegui la query utilizzando l'ID messaggio nel codice di esempio seguente.

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

Questo deve anche restituire il messaggio ricevuto, perché l'ID messaggio è identico. Utilizza l'ID di tracciamento nel codice di esempio per eseguire query sul recapito.

```
fields @timestamp, event.eventName
```

```
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

Questo codice restituisce l'operazione di recapito e le eventuali operazioni delle regole applicabili.

Example Visualizza tutta la posta ricevuta da un utente o da un dominio

Il codice di esempio seguente illustra come eseguire query su tutta la posta ricevuta da un utente specificato.

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

Il codice di esempio seguente illustra come eseguire query su tutta la posta ricevuta da un dominio specificato.

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

Example Scopri chi ha inviato le email respinte

Il codice di esempio seguente illustra come eseguire query per e-mail in uscita che non sono state recapitate, inoltre restituisce i motivi del mancato recapito.

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

Il seguente esempio di codice mostra come eseguire una query per le e-mail in arrivo che sono state respinte. Restituisce inoltre gli indirizzi e-mail dei destinatari respinti e i motivi del rifiuto.

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason,
 event.bouncedRecipient.status
| sort @timestamp desc
```

```
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

Example Scopri quali domini inviano spam

Il codice di esempio seguente illustra come eseguire query su destinatari nell'organizzazione che ricevono posta indesiderata.

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

Il codice di esempio seguente illustra come eseguire query sul mittente delle e-mail di spam.

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

Example Scopri perché un'email è stata inviata alla cartella spam di un destinatario

Il codice di esempio seguente illustra come eseguire query su e-mail identificate come spam, filtrate in base all'oggetto.

```
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"
```

Puoi inoltre possibile eseguire query in base all'ID di tracciamento e-mail per visualizzare tutti gli eventi per l'e-mail.

Example Visualizza le e-mail che corrispondono alle regole del flusso di posta elettronica

Il codice di esempio seguente illustra come eseguire query su e-mail che soddisfano le regole del flusso di e-mail in uscita.

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

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

Il codice di esempio seguente illustra come eseguire query su e-mail che soddisfano le regole del flusso di e-mail in entrata.

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

Example Scopri quante email vengono ricevute o inviate dalla tua organizzazione

Il codice di esempio seguente illustra come eseguire query sul numero di e-mail ricevute da ogni destinatario nell'organizzazione.

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

Il codice di esempio seguente illustra come eseguire query sul numero di e-mail inviate da ogni mittente nell'organizzazione.

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

Registrazione delle chiamate WorkMail API Amazon con AWS CloudTrail

Amazon WorkMail è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS in Amazon WorkMail. CloudTrail acquisisce tutte le chiamate API per Amazon WorkMail come eventi, incluse le chiamate dalla WorkMail console Amazon e le chiamate in codice verso Amazon WorkMail APIs. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon. WorkMail Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata ad Amazon WorkMail, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

WorkMail Informazioni su Amazon in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Amazon WorkMail, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon WorkMail, devi creare un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consultare:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le WorkMail azioni di Amazon vengono registrate CloudTrail e documentate nell'Amazon WorkMail API Reference. Ad esempio, le chiamate alle operazioni API `CreateUser`, `CreateAlias` e `GetRawMessageContent` generano voci nei file di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprendere le voci dei file di WorkMail log di Amazon

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta da qualsiasi sorgente e include informazioni sull'azione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log di CloudTrail non sono una traccia di stack ordinata delle chiamate API pubbliche, pertanto non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`CreateUser`azione dell' WorkMail API Amazon.

```
{
  "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"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`CreateAlias`azione dell' WorkMail API Amazon.

```
{
  "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"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che mostra l'`GetRawMessageContent`azione dell'API Amazon WorkMail Message Flow.

```
{
  "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"
}
```

Abilitazione della registrazione degli eventi via e-mail

Abilita la registrazione degli eventi e-mail nella WorkMail console Amazon per tenere traccia dei messaggi e-mail per la tua organizzazione. La registrazione degli eventi e-mail utilizza un ruolo AWS Identity and Access Management collegato al servizio (SLR) per concedere le autorizzazioni per pubblicare i registri degli eventi e-mail su Amazon. CloudWatch Per ulteriori informazioni sui ruoli collegati ai servizi IAM, consulta. Utilizzo di ruoli collegati ai servizi per Amazon WorkMail

Nei registri degli CloudWatch eventi, puoi utilizzare strumenti e metriche di CloudWatch ricerca per tenere traccia dei messaggi e risolvere i problemi relativi alle e-mail. Per ulteriori informazioni sui registri degli eventi a cui Amazon WorkMail invia CloudWatch, consultaMonitoraggio dei registri degli eventi WorkMail e-mail di Amazon. Per ulteriori informazioni sui CloudWatch log, consulta la Amazon CloudWatch Logs User Guide.

Argomenti

- Per disattivare la registrazione degli eventi e-mail
- Creazione di un gruppo di log personalizzato e di un ruolo IAM per la registrazione degli eventi via e-mail
- Per disattivare la registrazione degli eventi e-mail
- Prevenzione del confused deputy tra servizi

Per disattivare la registrazione degli eventi e-mail

Quando attivi la registrazione degli eventi e-mail utilizzando le impostazioni predefinite, Amazon WorkMail, si verifica quanto segue:

- Crea un ruolo AWS Identity and Access Management collegato al servizio —. `AmazonWorkMailEvents`
- Crea un gruppo di CloudWatch log —. `/aws/workmail/emailevents/`*`organization-alias`*
- Imposta la conservazione dei CloudWatch log su 30 giorni.

Per attivare la registrazione degli eventi e-mail

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Impostazioni di registrazione.
4. Scegli la scheda Impostazioni del registro del flusso di posta elettronica.
5. Nella sezione Impostazioni del registro del flusso di posta elettronica, scegli Modifica.
6. Sposta il cursore Abilita eventi di posta elettronica in posizione Attiva.
7. Esegui una di queste operazioni:

   - (Consigliato) Scegliete Usa impostazioni predefinite.
   - (Facoltativo) Cancella le impostazioni Use default e seleziona un gruppo di log di destinazione e un ruolo IAM dagli elenchi visualizzati.

   > **Note**
   >
   > Scegli questa opzione solo se hai già creato un gruppo di log e un ruolo IAM personalizzato utilizzando AWS CLI. Per ulteriori informazioni, consulta Creazione di un gruppo di log personalizzato e di un ruolo IAM per la registrazione degli eventi via e-mail.

8. Seleziona Autorizzo Amazon WorkMail a pubblicare i log nel mio account utilizzando questa configurazione.
9. Seleziona Salva.

Creazione di un gruppo di log personalizzato e di un ruolo IAM per la registrazione degli eventi via e-mail

Ti consigliamo di utilizzare le impostazioni predefinite quando abiliti la registrazione degli eventi e-mail per Amazon WorkMail. Se hai bisogno di una configurazione di monitoraggio personalizzata, puoi utilizzare la AWS CLI per creare un gruppo di log dedicato e un ruolo IAM personalizzato per la registrazione degli eventi via e-mail.

Per creare un gruppo di log personalizzato e un ruolo IAM per la registrazione degli eventi via e-mail

1. Usa il seguente AWS CLI comando per creare un gruppo di log nella stessa AWS regione della tua WorkMail organizzazione Amazon. Per ulteriori informazioni, consulta la sezione create-log-group nella Documentazione di riferimento della AWS CLI .

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

2. Creare un file contenente la seguente policy:

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

3. Utilizza il AWS CLI comando seguente per creare un ruolo IAM e allegare questo file come documento relativo alla politica del ruolo. Per ulteriori informazioni, consulta create-role nella Guida di riferimento ai comandi di AWS CLI .

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

> **Note**
>
> Se sei un utente di policy `WorkMailFullAccess` gestite, devi includere il termine `workmail` nel nome del ruolo. Questa policy gestita consente solo di configurare la registrazione degli eventi e-mail utilizzando i ruoli con `workmail` nel nome. Per ulteriori informazioni, consulta Concedere a un utente le autorizzazioni per passare un ruolo a un AWS servizio nella Guida per l'utente IAM.

4. Crea un file contenente la policy per il ruolo IAM che hai creato nel passaggio precedente. La policy deve concedere al ruolo almeno le autorizzazioni per creare flussi di log e inserire gli eventi di log nel gruppo di log creato al passaggio 1.

```
{
    "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. Utilizza il AWS CLI comando seguente per allegare il file di policy al ruolo IAM. Per ulteriori informazioni, consulta la sezione put-role-policy nella Documentazione di riferimento della AWS CLI .

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

Per disattivare la registrazione degli eventi e-mail

Disattiva la registrazione degli eventi e-mail dalla WorkMail console Amazon. Se non hai più bisogno di utilizzare la registrazione degli eventi via e-mail, ti consigliamo di eliminare anche il gruppo di CloudWatch log correlato e il ruolo collegato al servizio. Per ulteriori informazioni, consulta Eliminazione di un ruolo collegato al servizio per Amazon WorkMail.

Per disattivare la registrazione degli eventi e-mail

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Monitoring (Monitoraggio).
4. Nella sezione Impostazioni del registro, scegli Modifica.
5. Sposta il cursore Abilita eventi di posta elettronica in posizione OFF.
6. Seleziona Salva.

Prevenzione del confused deputy tra servizi

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato).

Il servizio di chiamata può essere manipolato in modo da utilizzare le sue autorizzazioni per agire su risorse di un altro cliente a cui altrimenti non avrebbe l'autorizzazione di accedere.

Per evitare che ciò accada, AWS mette a disposizione strumenti che consentono di proteggere i dati relativi a tutti i servizi con responsabili del servizio a cui è stato concesso l'accesso alle risorse del vostro account.

Consigliamo di utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition nelle politiche delle risorse per limitare le autorizzazioni concesse da CloudWatch Logs e

Amazon S3 ai servizi che generano i log. Se utilizzi entrambe le chiavi di contesto della condizione globale, i valori devono utilizzare lo stesso ID account quando vengono utilizzati nella stessa dichiarazione politica.

I valori di `aws:SourceArn` devono essere quelli ARNs delle fonti di consegna che generano i log.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o se si sta specificando più risorse, utilizzare la chiave di condizione del contesto globale `aws:SourceArn` con caratteri speciali (`*`) per le parti sconosciute dell'ARN.

Abilitazione della registrazione di controllo

Puoi utilizzare i log di controllo per acquisire informazioni dettagliate sull'utilizzo della tua WorkMail organizzazione Amazon. I log di controllo possono essere utilizzati per monitorare l'accesso degli utenti alle caselle di posta, verificare la presenza di attività sospette ed eseguire il debug del controllo degli accessi e delle configurazioni dei provider di disponibilità.

> **Note**
>
> La politica AmazonWorkMailFullAccessgestita non include tutte le autorizzazioni necessarie per gestire le consegne dei log. Se utilizzi questa politica per la gestione WorkMail, assicurati che il principale (ad esempio, il ruolo assunto) utilizzato per configurare le consegne dei log disponga anche di tutte le autorizzazioni richieste.

Amazon WorkMail supporta tre destinazioni di consegna per i log di controllo: CloudWatch Logs, Amazon S3 e Amazon Data Firehose. Per ulteriori informazioni, consulta la sezione Registrazione che richiede autorizzazioni aggiuntive [V2] nella Amazon CloudWatch Logs User Guide.

Oltre alle autorizzazioni elencate in Registrazione che richiede autorizzazioni aggiuntive [V2], Amazon WorkMail richiede un'autorizzazione aggiuntiva per configurare la consegna dei log:. `workmail:AllowVendedLogDeliveryForResource`

Una consegna di log funzionante è composta da tre elementi:

- DeliverySource, un oggetto logico che rappresenta la risorsa o le risorse che inviano i log. Per Amazon WorkMail, è l' WorkMailorganizzazione Amazon.
- A DeliveryDestination, che è un oggetto logico che rappresenta l'effettiva destinazione di consegna.

- Una consegna, che collega una fonte di consegna alla destinazione di consegna.

Per configurare la consegna dei log tra Amazon WorkMail e una destinazione, puoi fare quanto segue:

- Crea una fonte di consegna con PutDeliverySource.
- Crea una destinazione di consegna con PutDeliveryDestination.
- Se stai distribuendo log su più account, devi utilizzarli PutDeliveryDestinationPolicynell'account di destinazione per assegnare una policy IAM alla destinazione. Questa policy autorizza la creazione di una consegna dalla fonte di consegna nell'account A alla destinazione di consegna nell'account B.
- Crea una consegna associando esattamente una fonte di consegna e una destinazione di consegna utilizzando. CreateDelivery

Le sezioni seguenti forniscono i dettagli delle autorizzazioni di cui devi disporre quando effettui l'accesso per configurare la consegna dei log a ciascun tipo di destinazione. Queste autorizzazioni possono essere concesse a un ruolo IAM con cui hai effettuato l'accesso.

> **Important**
>
> È tua responsabilità rimuovere le risorse di distribuzione dei log dopo aver eliminato la risorsa che genera i log.

Per rimuovere le risorse di consegna dei log dopo aver eliminato la risorsa che genera i log, segui questi passaggi.

1. Eliminare la consegna utilizzando l'operazione. DeleteDelivery
2. Eliminare il DeliverySourceutilizzando l'DeleteDeliverySourceoperazione.
3. Se l'DeliveryDestinationelemento associato a DeliverySourcequello che hai appena eliminato viene utilizzato solo per questo specifico DeliverySource, puoi rimuoverlo utilizzando l'DeleteDeliveryDestinationsoperazione.

Configurazione della registrazione di controllo tramite la console Amazon WorkMail

Puoi configurare la registrazione di controllo nella WorkMail console Amazon:

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e seleziona una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Scegli Impostazioni di registrazione.
4. Scegli la scheda Impostazioni del registro di controllo.
5. Configura le consegne per il tipo di registro richiesto utilizzando il widget appropriato.
6. Seleziona Salva.

Registri inviati a Logs CloudWatch

Autorizzazioni degli utenti

Per abilitare l'invio dei log ai CloudWatch registri, è necessario accedere con le seguenti autorizzazioni.

```
{
    "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"
            ]
        }
    ]
}
```

Policy delle risorse del gruppo di log

Il gruppo di log in cui vengono inviati i log deve disporre di una policy delle risorse che includa determinate autorizzazioni. Se al momento il gruppo di log non dispone di una politica in materia di risorse e l'utente che configura la `logs:PutResourcePolicy` registrazione dispone `logs:DescribeLogGroups` delle autorizzazioni relative al gruppo di log, crea AWS automaticamente la seguente politica quando si inizia a inviare i log a Logs. `logs:DescribeResourcePolicies` CloudWatch

```
{
    "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:*"
                    ]
                }
            }
        }
    ]
}
```

Considerazioni relative al limite delle dimensioni delle policy delle risorse del gruppo di log

Questi servizi devono elencare ogni gruppo di log a cui inviano i log nella politica delle risorse. CloudWatch Le politiche relative alle risorse dei log sono limitate a 5.120 caratteri. Un servizio che invia log a un gran numero di gruppi di log potrebbe raggiungere questo limite.

Per mitigare questo problema, CloudWatch Logs monitora la dimensione delle politiche relative alle risorse utilizzate dal servizio che invia i log. Quando rileva che una policy si avvicina al limite di dimensione di 5.120 caratteri, CloudWatch Logs `/aws/vendedlogs/*` abilita automaticamente la politica delle risorse per quel servizio. Quindi puoi iniziare a utilizzare gruppi di log con nomi che iniziano con `/aws/vendedlogs/` come destinazioni per i log di questi servizi.

Log inviati ad Amazon S3

Autorizzazioni degli utenti

Per abilitare l'invio di log ad Amazon S3, devi aver effettuato l'accesso con le seguenti autorizzazioni.

```
{
    "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"
            ]
        }
    ]
}
```

Il bucket S3 in cui vengono inviati i log deve disporre di una policy delle risorse che include determinate autorizzazioni. Se il bucket attualmente non dispone di una politica delle risorse e l'utente che configura la registrazione dispone delle autorizzazioni `S3:GetBucketPolicy` e `S3:PutBucketPolicy` delle autorizzazioni per il bucket, crea AWS automaticamente la seguente politica quando inizi a inviare i log ad Amazon S3.

```
{
    "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:*"
                    ]
                }
            }
        }
    ]
```

```
}
```

Nella politica precedente, per`aws:SourceAccount`, specifica l'elenco degli account IDs per i quali i log vengono consegnati a questo bucket. Per`aws:SourceArn`, specifica l'elenco ARNs della risorsa che genera i log, nel modulo. `arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`

Se il bucket ha una politica in materia di risorse, ma tale politica non contiene l'istruzione mostrata nella politica precedente e l'utente che configura la registrazione dispone delle `S3:PutBucketPolicy` autorizzazioni `S3:GetBucketPolicy` e per il bucket, tale istruzione viene aggiunta alla politica delle risorse del bucket.

> **Note**
>
> In alcuni casi, potresti riscontrare `AccessDenied` degli errori AWS CloudTrail se l'`s3:ListBucket`autorizzazione non è stata concessa a. `delivery.logs.amazonaws.com` Per evitare questi errori nei CloudTrail registri, devi concedere l'`s3:ListBucket`autorizzazione a`delivery.logs.amazonaws.com`. È inoltre necessario includere i `Condition` parametri mostrati con l'`s3:GetBucketAcl`autorizzazione impostata nella precedente policy del bucket. Per semplificare questa operazione, invece di crearne uno nuovo`Statement`, puoi aggiornare direttamente il `AWSLogDeliveryAclCheck` tobe. `“Action”: [“s3:GetBucketAcl”, “s3:ListBucket”]`

Crittografia lato server di bucket Amazon S3

Puoi proteggere i dati nel tuo bucket Amazon S3 abilitando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) o la crittografia lato server con una chiave archiviata in (SSE-KMS). AWS KMS AWS Key Management Service Per ulteriori informazioni, consulta Protezione dei dati con la crittografia lato server.

Se si sceglie SSE-S3, non è richiesta alcuna configurazione aggiuntiva. Amazon S3 gestisce la chiave di crittografia.

> **Warning**
>
> Se scegli SSE-KMS, devi utilizzare una chiave gestita dal cliente, poiché l'utilizzo di una non è supportato in questo scenario. Chiave gestita da AWS Se si configura la crittografia utilizzando una chiave AWS gestita, i log verranno consegnati in un formato illeggibile.

Quando utilizzi una AWS KMS chiave gestita dal cliente, puoi specificare l'Amazon Resource Name (ARN) della chiave gestita dal cliente quando abiliti la crittografia dei bucket. Aggiungi quanto segue alla politica chiave per la tua chiave gestita dal cliente (non alla politica del bucket per il tuo bucket S3), in modo che l'account di consegna dei log possa scrivere sul tuo bucket S3.

Se scegli SSE-KMS, devi utilizzare una chiave gestita dal cliente, poiché l'utilizzo di una chiave gestita non è supportato in questo scenario AWS . Quando utilizzi una AWS KMS chiave gestita dal cliente, puoi specificare l'Amazon Resource Name (ARN) della chiave gestita dal cliente quando abiliti la crittografia dei bucket. Aggiungi quanto segue alla politica chiave per la tua chiave gestita dal cliente (non alla politica del bucket per il tuo bucket S3), in modo che l'account di consegna dei log possa scrivere sul tuo bucket S3.

```
{
    "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:*"
            ]
        }
    }
}
```

Per `aws:SourceAccount`, specifica l'elenco degli account IDs per i quali i log vengono consegnati a questo bucket. Per `aws:SourceArn`, specifica l'elenco ARNs della risorsa che genera i log, nel modulo. `arn:aws:logs:source-region:source-account-id:*`

Log inviati a Firehose

Autorizzazioni degli utenti

Per abilitare l'invio di log a Firehose, è necessario accedere con le seguenti autorizzazioni.

```
{
    "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"
            ]
        }
    ]
}
```

Ruoli IAM utilizzati per le autorizzazioni delle risorse

Poiché Firehose non utilizza policy relative alle risorse, AWS utilizza i ruoli IAM per configurare questi log da inviare a Firehose. AWS crea un ruolo collegato al servizio denominato AWSServiceRoleForLogDelivery. Questo ruolo collegato al servizio include le seguenti autorizzazioni.

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

Questo ruolo collegato al servizio concede l'autorizzazione per tutti i flussi di distribuzione Firehose con il tag impostato su. `LogDeliveryEnabled` `true` AWS assegna questo tag al flusso di consegna di destinazione quando si configura la registrazione.

Questo ruolo collegato al servizio dispone inoltre di una policy di attendibilità che autorizzi il principale del servizio `delivery.logs.amazonaws.com` di assumere il ruolo collegato al servizio necessario. Questa policy di attendibilità è la seguente:

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

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Autorizzazioni specifiche per la console

Oltre alle autorizzazioni elencate nelle sezioni precedenti, se stai configurando la consegna dei log utilizzando la console anziché il APIs, sono necessarie anche le seguenti autorizzazioni:

```
{
    "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":"*"
        }
    ]
}
```

Convalida della conformità per Amazon WorkMail

I revisori di terze parti valutano la sicurezza e la conformità di Amazon nell' WorkMail ambito di diversi programmi di AWS conformità. Sono inclusi SOC, ISO e C5.

Per un elenco di AWS servizi nell'ambito di programmi di conformità specifici, consulta AWS Services in Scope by Compliance Program. Per informazioni generali, consulta Programmi di conformità di AWS.

Puoi scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta l'argomento Download dei rapporti in AWS Artifact.

La tua responsabilità di conformità quando usi Amazon WorkMail è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità della tua azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono i passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- AWS Risorse per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Config— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente AWS di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in Amazon WorkMail

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni offrono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Amazon WorkMail offre diverse funzionalità per aiutarti a supportare le tue esigenze di resilienza e backup dei dati.

Sicurezza dell'infrastruttura in Amazon WorkMail

> **Note**
>
> Amazon WorkMail ha interrotto il supporto per Transport Layer Security (TLS) 1.0 e 1.1. Se utilizzi TLS 1.0 o 1.1, devi aggiornare la versione TLS alla 1.2. Per ulteriori informazioni, consulta TLS 1.2 per diventare il livello minimo di protocollo TLS per tutti gli endpoint delle API AWS.

In quanto servizio gestito, Amazon WorkMail è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon WorkMail tramite la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Guida introduttiva ad Amazon WorkMail

Dopo aver completato ilPrerequisiti, sei pronto per iniziare a usare Amazon WorkMail. Per ulteriori informazioni, consulta Guida introduttiva ad Amazon WorkMail.

Puoi saperne di più sulla migrazione delle caselle di posta esistenti su Amazon WorkMail, sull'interoperabilità con Microsoft Exchange e sulle quote WorkMail Amazon nelle sezioni seguenti.

Argomenti

Guida introduttiva ad Amazon WorkMail

Che tu sia un nuovo WorkMail utente Amazon o un utente esistente di Amazon WorkSpaces, inizia a usare Amazon WorkMail completando i seguenti passaggi.

> **Note**
>
> Completa i Prerequisiti prima di iniziare.

Argomenti

Passaggio 1: accedi alla WorkMail console Amazon

Devi accedere alla WorkMail console Amazon prima di poter aggiungere utenti e gestirne account e caselle di posta.

Per accedere alla WorkMail console Amazon

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.
2. Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni sulle regioni, consulta Regioni ed endpoint in. Riferimenti generali di Amazon Web Services

Passaggio 2: configura il tuo WorkMail sito Amazon

1. Dopo aver effettuato l'accesso alla WorkMail console Amazon, configuri la tua organizzazione e aggiungi un dominio. Ti consigliamo di utilizzare un dominio dedicato per la tua WorkMail organizzazione Amazon. Per ulteriori informazioni, consultare Creazione di un'organizzazione e Aggiunta di un dominio.
2. (Facoltativo) Puoi scegliere di utilizzare un dominio di prova gratuito fornito da Amazon WorkMail. Se scegli di farlo, vai al passaggio 4.

   > **Note**
   >
   > I domini di test utilizzano questo formato: *alias* .awsapps.com. Mentre procedi, ricorda che dovresti usare solo i domini di test per i test. Non utilizzare un dominio di test per un ambiente di produzione. Inoltre, devi avere almeno un utente abilitato nella tua WorkMail organizzazione Amazon. Se non disponi di un utente abilitato, il dominio può diventare disponibile per la registrazione e l'uso da parte di altri clienti.

3. Se utilizzi un dominio esterno, verifica tale dominio aggiungendo i record di testo (TXT) e di scambio di posta (MX) appropriati al servizio Domain Name System (DNS). I record TXT consentono di inserire note nel DNS. I record MX specificano i server di posta in arrivo. Assicurati

di impostare il dominio come predefinito per la tua organizzazione. Per ulteriori informazioni, consultare Verifica dei domini e Selezione del dominio predefinito.

4. Crea nuovi utenti o abilita gli utenti della directory esistenti per Amazon WorkMail. Per ulteriori informazioni, consulta Aggiunta di un utente.
5. (Facoltativo) Se disponi di caselle di posta Microsoft Exchange esistenti, eseguine la migrazione su Amazon. WorkMail Per ulteriori informazioni, consulta Migrazione ad Amazon WorkMail.

Dopo aver completato la configurazione del tuo WorkMail sito Amazon, puoi accedere ad Amazon WorkMail utilizzando l'URL dell'applicazione Web.

Per individuare l'URL della tua applicazione WorkMail web Amazon

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. A tale scopo, apri l'elenco Seleziona una regione, situato a destra della casella di ricerca, quindi scegli la regione desiderata. Per ulteriori informazioni, consulta Regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.

   Viene visualizzata la pagina delle impostazioni dell'organizzazione che mostra l'URL in Accesso utente. URLs Prendi questo modulo: https://*alias*.awsapps.com/mail.

Passaggio 3: configurare WorkMail l'accesso utente Amazon

Scegli tra le seguenti opzioni per configurare WorkMail l'accesso degli utenti Amazon:

- Configurare l'accesso utente da un client per desktop esistente utilizzando il client Microsoft Outlook. Per ulteriori informazioni, consulta Connect Microsoft Outlook al tuo WorkMail account Amazon.
- Configura l'accesso utente da un dispositivo mobile, come Kindle, Android, iPad o iPhone. Per ulteriori informazioni, consulta Nozioni di base su un dispositivo mobile.
- Per configurare l'accesso utente, utilizza qualsiasi software client compatibile con il protocollo Internet Mail Access Protocol (IMAP). Per ulteriori informazioni, consulta Connect IMAP client al tuo WorkMail account Amazon.

Altre risorse

- Migrazione ad Amazon WorkMail
- Interoperabilità tra Amazon e WorkMail Microsoft Exchange
- WorkMail Quote Amazon

Migrazione ad Amazon WorkMail

Puoi migrare ad Amazon WorkMail da Microsoft Exchange, Microsoft Office 365, G Suite Basic (precedentemente Google Apps for Work) e altre piattaforme collaborando con uno dei nostri partner. Per ulteriori informazioni sui nostri partner, consulta Amazon WorkMail Features.

Argomenti

- Passaggio 1: creare o abilitare gli utenti in Amazon WorkMail
- Fase 2: Migrazione ad Amazon WorkMail
- Fase 3: Completa la migrazione ad Amazon WorkMail

Passaggio 1: creare o abilitare gli utenti in Amazon WorkMail

Prima di migrare i tuoi utenti, devi aggiungerli in Amazon WorkMail per effettuare il provisioning della loro casella di posta. Per ulteriori informazioni, consulta Aggiunta di un utente.

Fase 2: Migrazione ad Amazon WorkMail

Puoi collaborare con qualsiasi partner di AWS migrazione per migrare ad Amazon WorkMail. Per informazioni su questi provider, consulta le WorkMailfunzionalità di Amazon.

Per migrare le tue caselle di posta, crea un WorkMail utente Amazon dedicato che funga da amministratore della migrazione. La procedura seguente concede a quell'utente l'autorizzazione ad accedere a tutte le cassette postali della tua organizzazione.

Per creare un amministratore della migrazione

1. Esegui una di queste operazioni:

   - Nella WorkMail console Amazon, crea un nuovo utente che funga da amministratore della migrazione. Per ulteriori informazioni, consulta Aggiunta di un utente.

- In Active Directory, crea un nuovo utente che funga da amministratore della migrazione, quindi abilita l'utente per Amazon WorkMail. Per ulteriori informazioni, consulta Abilitare gli utenti.

2. Nel riquadro di navigazione della WorkMail console Amazon, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Scegli Impostazioni dell'organizzazione, scegli Migrazione, quindi Modifica.
4. Sposta il cursore abilitato alla migrazione in posizione Attiva.
5. Apri l'amministratore della migrazione e seleziona un utente.
6. Scegli Save (Salva).

Fase 3: Completa la migrazione ad Amazon WorkMail

Dopo aver migrato i tuoi account e-mail su Amazon WorkMail, puoi verificare i tuoi record DNS e configurare i client desktop e mobili.

Per completare la migrazione ad Amazon WorkMail

1. Verifica che tutti i record DNS siano aggiornati e che puntino ad Amazon WorkMail. Per maggiori informazioni sui record DNS richiesti, consultare Aggiunta di un dominio.

   > **Note**
   >
   > Il processo di aggiornamento dei record DNS può richiedere diverse ore. Se nuovi elementi vengono visualizzati in una casella di posta di origine mentre i record MX sono in fase di modifica, eseguire nuovamente lo strumento di migrazione per migrare i nuovi elementi dopo l'aggiornamento dei record DNS.

2. Per ulteriori informazioni sulla configurazione dei client desktop o mobili per l'utilizzo di Amazon WorkMail, consulta Connect Microsoft Outlook al tuo WorkMail account Amazon nella Amazon WorkMail User Guide.

Interoperabilità tra Amazon e WorkMail Microsoft Exchange

L'interoperabilità tra Amazon e WorkMail Microsoft Exchange Server consente di ridurre al minimo le interruzioni per gli utenti durante la migrazione delle caselle di posta su Amazon WorkMail o l'utilizzo di Amazon WorkMail per un sottoinsieme delle caselle di posta aziendali.

Tale interoperabilità consente di utilizzare lo stesso dominio aziendale per le caselle di posta in entrambi gli ambienti. In questo modo, gli utenti possono pianificare riunioni con la condivisione bidirezionale delle informazioni sullo stato di disponibilità e disponibilità del calendario.

Prerequisiti

Prima di abilitare l'interoperabilità con Microsoft Exchange, completa le seguenti operazioni:

- Assicurati di avere almeno un utente abilitato per Amazon. WorkMail È necessario per configurare le impostazioni di disponibilità per Microsoft Exchange. Per abilitare un utente, segui le istruzioni su Abilitare il routing di e-mail per un utente.
- Configura un Active Directory (AD) Connector. La configurazione di un AD Connector con la directory locale consente agli utenti di continuare a utilizzare le credenziali aziendali esistenti. Per ulteriori informazioni, consulta Creare un connettore AD e integrare Amazon WorkMail con la tua directory locale.
- Configura la tua WorkMail organizzazione Amazon. Crea un' WorkMail organizzazione Amazon che utilizzi l'AD Connector che hai configurato.
- Aggiungi i domini aziendali alla tua WorkMail organizzazione Amazon e verificali nella WorkMail console Amazon. In caso contrario, le e-mail inviate a questo alias non saranno recapitate. Per ulteriori informazioni sull'utilizzo dei domini, consulta l'argomento relativo all'utilizzo dei domini.
- Migra le caselle di posta su Amazon WorkMail. Consenti agli utenti di effettuare il provisioning e migrare le caselle di posta dal tuo ambiente locale ad Amazon. WorkMail Per ulteriori informazioni, consulta Abilitare gli utenti esistenti e vedere Migrazione ad Amazon WorkMail.

  > **Note**
  >
  > Non aggiornare i record DNS in modo che indirizzino ad Amazon WorkMail. In questo modo Microsoft Exchange rimane impostato come server principale per le e-mail in entrata per il tempo che si desidera disporre dell'interoperabilità tra i due ambienti.

- Assicurati che i nomi dei principali utenti (UPNs) in Active Directory corrispondano agli indirizzi SMTP primari degli utenti.

Amazon invia WorkMail richieste HTTPS all'URL di Exchange Web Services (EWS) su Microsoft Exchange per ottenere informazioni sulla disponibilità o sull'occupazione del calendario.

Per i provider di disponibilità basati su EWS, Amazon WorkMail effettua richieste HTTPS all'URL di Exchange Web Services (EWS) su Microsoft Exchange per ottenere informazioni sulla disponibilità del calendario. Pertanto, i seguenti prerequisiti si applicano solo ai provider di disponibilità basati su EWS.

- Assicuratevi che le impostazioni del firewall pertinenti siano configurate per consentire l'accesso da Internet. La porta predefinita per le richieste HTTPS è la porta 443.
- Amazon WorkMail può effettuare richieste HTTPS con successo all'URL EWS su Microsoft Exchange solo quando nel tuo ambiente Microsoft Exchange è disponibile un certificato firmato da un'autorità di certificazione (CA) valida. Per ulteriori informazioni, vedere Creare una richiesta di certificato Exchange Server per un'autorità di certificazione sul sito Web della documentazione di Microsoft Exchange.
- È necessario abilitare l'autenticazione di base per EWS in Microsoft Exchange. Per ulteriori informazioni consulta l'argomento relativo a Virtual Directories: Exchange 2013 sul sito Microsoft MVP Award Program Blog.

Aggiungere domini e abilitare caselle di posta

Aggiungi i tuoi domini aziendali ad Amazon WorkMail in modo che possano essere utilizzati negli indirizzi e-mail. Assicurati che i domini aggiunti ad Amazon WorkMail siano verificati, quindi consenti a utenti e gruppi di effettuare il provisioning delle caselle di posta su Amazon. WorkMail Le risorse non possono essere abilitate in Amazon WorkMail in modalità di interoperabilità e devono essere ricreate in Amazon WorkMail dopo aver disabilitato la modalità di interoperabilità. È comunque possibile utilizzarle per pianificare riunioni mentre in modalità di interoperabilità. Le risorse di Microsoft Exchange vengono sempre visualizzate nella scheda Utenti di Amazon WorkMail.

- Per ulteriori informazioni, consulta gli argomenti relativi all'aggiunta di domini, all'abilitazione degli utenti esistenti e all'abilitazione di gruppi esistenti.

> **Note**
>
> Per garantire l'interoperabilità con Microsoft Exchange, non aggiornare i record DNS in modo che rimandino ai record Amazon. WorkMail Microsoft Exchange rimane impostato come server principale per le e-mail in entrata per il tempo che si desidera disporre dell'interoperabilità tra i due ambienti.

Abilitare l'interoperabilità.

Se non hai creato un' WorkMail organizzazione Amazon, puoi utilizzare l'API pubblica per creare una nuova WorkMail organizzazione con la modalità di interoperabilità abilitata.

Se hai già un' WorkMail organizzazione Amazon con un AD Connector collegato ad Active Directory e disponi anche di Microsoft Exchange, contatta AWS Support per ricevere assistenza su come abilitare l'interoperabilità di Microsoft Exchange per un'organizzazione Amazon WorkMail esistente.

Crea account di servizio in Microsoft Exchange e Amazon WorkMail

> **Note**
>
> La creazione di un account di servizio in Exchange non è richiesta quando Exchange non viene utilizzato come back-end per un provider di disponibilità personalizzato.

Per accedere alle 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 informazioni del calendario di altri utenti di Exchange. L'accesso viene concesso per impostazione predefinita, pertanto non è richiesta alcuna autorizzazione speciale.

Allo stesso modo, l'account del WorkMail servizio Amazon è qualsiasi utente su Amazon WorkMail che ha accesso alle informazioni sulla disponibilità del calendario di altri utenti Amazon WorkMail . Anche in questo caso l'accesso è concesso per impostazione predefinita. Devi creare l' WorkMail utente Amazon nella tua directory locale, quindi abilitarlo per Amazon WorkMail, per integrare Amazon WorkMail con AD Connector nella tua directory.

Limitazioni nella modalità di interoperabilità

Quando l'organizzazione è in modalità di interoperabilità, è necessario utilizzare l'interfaccia di amministrazione di Exchange per gestire tutti gli utenti, i gruppi e le risorse. Per abilitare WorkMail utenti e gruppi Amazon, usa il AWS Management Console. Per ulteriori informazioni, consulta gli argomenti relativi all'abilitazione di utenti esistenti e all'abilitazione di gruppi esistenti.

Quando abiliti un utente o un gruppo per Amazon WorkMail, non puoi modificare gli indirizzi e-mail o gli alias di tali utenti e gruppi. Questi devono essere configurati anche tramite l'admincenter di Exchange. Amazon WorkMail sincronizza le modifiche nella tua directory ogni quattro ore.

Le risorse non possono essere create o abilitate in Amazon in WorkMail modalità di interoperabilità. Tuttavia, tutte le risorse di Exchange sono disponibili nella WorkMail rubrica di Amazon e possono essere utilizzate per pianificare le riunioni come al solito.

Configurare le impostazioni di disponibilità su Amazon WorkMail

Configura le impostazioni di disponibilità su Amazon WorkMail per consentire l'interrogazione di sistemi esterni, offrire funzionalità di calendario e ottenere free/busy information. Amazon WorkMail supports two modes of obtaining free/busy informazioni sul calendario da un sistema remoto:

- Exchange Web Services (EWS): in questa configurazione, Amazon WorkMail interrogherà un server Exchange o un'altra WorkMail organizzazione per ottenere informazioni sulla disponibilità utilizzando il protocollo EWS. Questa è la configurazione più semplice, ma richiede che l'endpoint EWS del server Exchange sia accessibile tramite la rete Internet pubblica.
- Custom Availability Provider (CAP): in questa configurazione, un amministratore può configurare una funzione AWS Lambda per ottenere informazioni sulla disponibilità degli utenti per un determinato dominio di posta elettronica. A seconda della piattaforma del server di posta in uso, l'utilizzo di CAP con Amazon WorkMail offre i seguenti vantaggi:
  - Ottieni la disponibilità degli utenti da EWS interno senza dover aprire il WorkMail firewall.
  - Ottieni la disponibilità degli utenti da sistemi diversi da Exchange o non EWS, come Google Workspace (precedentemente noto come G Suite).

Argomenti

Configura un provider di disponibilità basato su EWS

Per configurare le impostazioni di disponibilità basate su EWS sulla console, completare la procedura seguente:

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. A tale scopo, apri l'elenco Seleziona una regione, situato a destra della casella di ricerca, quindi scegli la regione desiderata. Per ulteriori informazioni,

consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome di un'organizzazione.
3. Nel riquadro di navigazione, scegli Impostazioni dell'organizzazione, quindi scegli la scheda Interoperabilità.
4. Scegli Aggiungi configurazione di disponibilità, quindi inserisci le seguenti informazioni:
   - Tipo: seleziona EWS.
   - Dominio: il dominio per il quale WorkMail tenterà di richiedere informazioni sulla disponibilità utilizzando questa configurazione.
   - URL EWS: Amazon WorkMail interrogherà questo URL sull'endpoint EWS. Consulta la sezione Ottenere l'URL EWS di questa guida.
   - Indirizzo e-mail utente: l'indirizzo e-mail dell'utente che WorkMail verrà utilizzato per l'autenticazione sull'endpoint EWS.
   - Password: la password che WorkMail verrà utilizzata per l'autenticazione sull'endpoint EWS.
5. Scegli Save (Salva).

Ottenere l'URL EWS

Per ottenere l'URL EWS per Exchange utilizzando Microsoft Outlook, completare la procedura seguente:

1. Accedi a Microsoft Outlook su Windows per qualsiasi utente nell'ambiente Exchange.
2. Premi il tasto Ctrl e apri il menu contestuale (con il pulsante destro del mouse) sull'icona di Microsoft Outlook nella barra delle attività.
3. Scegliete Test E-mail AutoConfiguration.
4. Inserisci l'indirizzo e-mail di Microsoft Exchange dell'utente e la password e seleziona Test (Prova).
5. Nella finestra Risultati, copia il valore per l'Availability Service URL (URL del servizio di disponibilità).

Per ottenere l'URL EWS da utilizzare PowerShell, al PowerShell prompt, esegui il seguente comando:

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

Per ottenere l'URL EWS per Amazon WorkMail, cerca innanzitutto il dominio EWS nella sezione WorkMail Endpoints e quote Amazon. Inserisci l'URL EWS `https://"EWS domain"/EWS/Exchange.asmx` e sostituisci «dominio EWS» con il tuo dominio EWS.

Configurazione di un provider di disponibilità personalizzato

Per configurare un Custom Availability Provider (CAP), completare la seguente procedura:

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. A tale scopo, apri l'elenco Seleziona una regione, situato a destra della casella di ricerca, quindi scegli la regione desiderata.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome di un'organizzazione.
3. Nel pannello di navigazione, scegli Impostazioni dell'organizzazione, quindi scegli Interoperabilità.
4. Scegli Aggiungi configurazione di disponibilità, quindi inserisci le seguenti informazioni:

   - Tipo: seleziona CAP Lambda.
   - Dominio: il dominio per il quale WorkMail tenterà di interrogare le informazioni sulla disponibilità utilizzando questa configurazione.
   - ARN — L'ARN della funzione Lambda che fornirà le informazioni sulla disponibilità.

Per creare una funzione CAP Lambda, vedere. Creazione di una funzione Lambda del Custom Availability Provider

Creazione di una funzione Lambda del Custom Availability Provider

I Custom Availability Provider (CAPs) sono configurati con un protocollo di richiesta e risposta basato su JSON scritto in uno schema JSON ben definito. Una funzione Lambda analizzerà la richiesta e fornirà una risposta valida.

Argomenti

- Elementi di richiesta e risposta
- Concessione dell'accesso per
- Esempio di WorkMail utilizzo di una funzione CAP Lambda da parte di Amazon

Elementi di richiesta e risposta

Elementi della richiesta

Di seguito è riportato un esempio di richiesta utilizzata per configurare un CAP per un WorkMail utente Amazon:

```
{
    "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"
    }
}
```

Una richiesta è composta da tre sezioni: requester, mailboxes e window. Queste sono descritte nelle Window sezioni seguenti Richiedente e di questa guida. Caselle di posta

Richiedente

La sezione richiedente fornisce informazioni sull'utente che ha effettuato la richiesta originale ad Amazon WorkMail. CAPs usa queste informazioni per modificare il comportamento del provider. Ad esempio, questi dati possono essere utilizzati per impersonare lo stesso utente sul provider di disponibilità del backend oppure alcuni dettagli possono essere omessi dalla risposta.

Campo	Descrizione	Richiesto
`Email`	L'indirizzo email principale del richiedente.	Sì
`Username`	Il nome utente del richiedente.	Sì

Campo	Descrizione	Richiesto
`Organization`	L'ID dell'organizzazione del richiedente.	Sì
`UserID`	L'ID del richiedente.	Sì
`Origin`	L'indirizzo remoto della richiesta.	No
`Bearer`	Riservato per uso futuro.	No

Caselle di posta

La sezione delle caselle di posta contiene un elenco separato da virgole di indirizzi e-mail degli utenti per i quali vengono richieste informazioni sulla disponibilità.

Window

La sezione finestra contiene la finestra temporale per la quale vengono richieste le informazioni sulla disponibilità. Entrambi `startDate` `endDate` sono specificati in UTC e sono formattati secondo RFC 3339. Non è previsto che gli eventi vengano troncati. In altre parole, se un evento inizia prima del definito`StartDate`, verrà utilizzato l'inizio originale.

Elementi di risposta

Amazon WorkMail aspetterà 25 secondi per ricevere una risposta dalla funzione CAP Lambda. Dopo 25 secondi, Amazon WorkMail presumerà che la funzione non sia riuscita e genererà errori per le caselle di posta associate nella risposta EWS GetUserAvailability. Ciò non causerà il fallimento dell'intera GetUserAvailability operazione.

Di seguito è riportato un esempio di risposta tratto dalla configurazione definita all'inizio di questa sezione:

```
{
    "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"
    }]
}
```

Una risposta è composta da una singola sezione di caselle di posta che consiste in un elenco di cassette postali. Ogni cassetta postale per la quale è stata ottenuta correttamente la disponibilità è composta da tre sezioni: cassetta postale, eventi e orari di lavoro. Se il provider di disponibilità non è riuscito a ottenere le informazioni sulla disponibilità di una cassetta postale, la sezione è composta da due sezioni: casella di posta ed errore. Queste sono descritte nelle seguenti Errore sezioni Cassetta postaleEventi,Ore lavorative, Fuso orarioPeriodi lavorativi, e di questa guida.

Cassetta postale

La sezione mailbox è l'indirizzo e-mail dell'utente che si trova nella sezione delle caselle di posta della richiesta.

Eventi

La sezione eventi è un elenco di eventi che si verificano nella finestra richiesta. Ogni evento è definito con i seguenti parametri:

Campo	Descrizione	Richiesto
`startTime`	L'ora di inizio dell'evento in UTC e formattata secondo RFC 3339.	Sì
`endTime`	L'ora di fine dell'evento in UTC e formattata secondo RFC 3339.	Sì
`busyType`	Il tipo di evento occupato. Può essere `Busy`, `Free` o `Tentative` .	Sì
`details`	I dettagli dell'evento.	No
`details.subject`	L'oggetto dell'evento.	Sì
`details.location`	Il luogo dell'evento.	Sì
`details.instanceType`	Il tipo di istanza dell'even to. Può essere `Single_In stance` , `Recurring`	Sì

Campo	Descrizione	Richiesto
	`_Instance` o `Exception`.	
`details.isMeeting`	Un valore booleano per indicare se l'evento ha partecipanti.	Sì
`details.isReminderSet`	Un valore booleano per indicare se l'evento ha un promemoria impostato.	Sì
`details.isPrivate`	Un valore booleano per indicare se l'evento è impostato come privato.	Sì

Ore lavorative

La sezione WorkingHours contiene informazioni sull'orario di lavoro del proprietario della cassetta postale. Contiene due sezioni: fuso orario e WorkingPeriods.

Fuso orario

La sottosezione timezone descrive il fuso orario del proprietario della cassetta postale. È importante visualizzare correttamente l'orario di lavoro dell'utente quando il richiedente lavora in un fuso orario diverso. Il fornitore di disponibilità è tenuto a descrivere esplicitamente il fuso orario, anziché utilizzare un nome. L'utilizzo della descrizione standardizzata del fuso orario aiuta a evitare le discrepanze del fuso orario.

Campo	Descrizione	Richiesto
`name`	Il nome del fuso orario.	Sì
`bias`	L'offset predefinito dal GMT in minuti.	Sì
`standardTime`	L'inizio dell'ora solare per il fuso orario specificato.	No

Campo	Descrizione	Richiesto
`daylightTime`	L'inizio dell'ora legale per il fuso orario specificato.	No

È necessario definire entrambi `standardTime` o ometterli entrambi. `daylightTime` I campi nell'`daylightTime`oggetto `standardTime` and sono:

Campo	Descrizione	Valori consentiti
`offset`	L'offset rispetto all'offset predefinito in minuti.	N/A
`time`	L'ora in cui avviene la transizione tra l'ora solare e l'ora legale, specificata come. `hh:mm:ss`	N/A
`month`	Il mese in cui avviene il passaggio dall'ora solare all'ora legale.	`JAN`,`FEB`, `MAR`, `APR`, `JUN`, `JUL`, `AUG`, `SEP`, `OCT`, `NOV`, `DEC`
`week`	La settimana all'interno del mese specificato in cui avviene il passaggio dall'ora solare all'ora legale.	`FIRST`, `SECOND`, `THIRD`, `FOURTH`, `LAST`
`dayOfWeek`	Il giorno della settimana specificata in cui avviene il passaggio dall'ora solare all'ora legale.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Periodi lavorativi

La sezione WorkingPeriods contiene uno o più oggetti del periodo di lavoro. Ogni periodo definisce un inizio e una fine del giorno lavorativo per uno o più giorni.

Campo	Descrizione	Valori consentiti
`startMinutes`	L'inizio della giornata lavorativa in minuti a partire dalla mezzanotte.	N/A
`endMinutes`	Fine della giornata lavorativa, in minuti a partire dalla mezzanotte.	N/A
`days`	I giorni a cui si applica questo periodo.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Errore

Il campo di errore può contenere messaggi di errore arbitrari. La tabella seguente elenca una mappatura di codici noti su codici di errore EWS. Tutti gli altri messaggi verranno mappati su. `ERROR_FREE_BUSY_GENERATION_FAILED`

Valore	Codice di errore EWS	
`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`	

Concessione dell'accesso per

Esegui il seguente comando Lambda da AWS Command Line Interface ()AWS CLI. Questo comando aggiunge una politica delle risorse alla funzione Lambda che analizza il CAP. Questa funzione consente al servizio di WorkMail disponibilità Amazon di richiamare la tua funzione Lambda.

```
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
```

Nel comando, aggiungi i seguenti parametri dove indicato:

- *LAMBDA_REGION*— Nome della regione in cui viene distribuito CAP Lambda. Ad esempio, `us-east-1`.
- *CAP_FUNCTION_NAME*— Nome della funzione CAP Lambda.

> **Note**
>
> Può essere il nome, l'alias o l'ARN parziale o completo della funzione CAP Lambda.

- *WM_REGION*— Nome della regione in cui l' WorkMail organizzazione Amazon richiama la funzione Lambda.

> **Note**
>
> Solo le seguenti regioni sono disponibili per l'uso con CAP:
>
> - Stati Uniti orientali (Virginia settentrionale)
> - US West (Oregon)
> - Europa (Irlanda)

- *WM_ACCOUNT_ID*— L'ID dell'account dell'organizzazione.
- *ORGANIZATION_ID*— L'ID dell'organizzazione che richiama il CAP Lambda. Ad esempio, Org ID: m-934ebb9eb57145d0a6cab566ca81a21f.

> **Note**
>
> *LAMBDA_REGION*WM_REGIONe sarà diverso solo se sono necessarie chiamate interregionali. Se le chiamate interregionali non sono necessarie, saranno le stesse.

Esempio di WorkMail utilizzo di una funzione CAP Lambda da parte di Amazon

Per un esempio di WorkMail utilizzo da parte di Amazon di una funzione CAP Lambda per interrogare un endpoint EWS, consulta questa applicazione di AWS esempio nel repository Serverless applications for Amazon. WorkMail GitHub

Configurare le impostazioni di disponibilità di Microsoft Exchange

Per reindirizzare ad Amazon tutte le richieste di informazioni relative alla disponibilità del calendario per gli utenti abilitati WorkMail, configura uno spazio di indirizzi di disponibilità in Microsoft Exchange.

Usa il seguente PowerShell comando per creare lo spazio degli indirizzi:

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

Quando richiesto, inserisci le credenziali dell'account di WorkMail servizio Amazon. Il nome utente deve essere inserito come **domain\username** (ovvero,. ***orgname*.awsapps.com \workmail_service_account_*username*** Qui, ***orgname*** rappresenta il nome dell' WorkMail organizzazione Amazon. Per ulteriori informazioni, consulta Crea account di servizio in Microsoft Exchange e Amazon WorkMail.

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

Per ulteriori informazioni, vedere AvailabilityAddressSpaceAdd-on Microsoft Docs.

Abilita il routing delle e-mail tra gli utenti di Microsoft Exchange e Amazon WorkMail

Con il routing delle e-mail tra Microsoft Exchange Server e Amazon WorkMail, gli utenti possono mantenere gli indirizzi e-mail esistenti dopo la migrazione ad Amazon. WorkMail Il routing della posta

elettronica consente di mantenere Microsoft Exchange Server come server SMTP (Simple Mail Transfer Protocol) principale per la posta in arrivo dell'organizzazione.

Prima di utilizzare il routing della posta elettronica, è necessario completare i seguenti prerequisiti:

- Abilita la modalità di interoperabilità per la tua organizzazione. Per ulteriori informazioni, consulta Abilitare l'interoperabilità..
- Assicurati di vedere il tuo dominio nella WorkMail console Amazon.
- Verifica che il nostro Microsoft Exchange Server sia in grado di inviare e-mail a Internet. Potrebbe essere necessario configurare un connettore di invio. Per ulteriori informazioni sui connettori di invio, vedere Creare un connettore di invio in Exchange Server per inviare posta a Internet nella documentazione Microsoft.

Abilitare il routing di e-mail per un utente

Si consiglia di completare i seguenti passaggi per gli utenti di prova prima di applicare qualsiasi modifica all'organizzazione.

1. Abilita l'account utente che stai migrando ad Amazon WorkMail. Per ulteriori informazioni, consulta l'argomento relativo all'abilitazione di utenti esistenti.
2. Nella WorkMail console Amazon, assicurati che ci siano almeno due indirizzi e-mail associati all'utente abilitato.
   - <*workmailuser*@ *orgname* .awsapps.com> (viene aggiunto automaticamente e può essere utilizzato per i test senza Microsoft Exchange).
   - <*workmailuser*@ *yourdomain* .com> (viene aggiunto automaticamente ed è l'indirizzo principale di Microsoft Exchange).

     Per ulteriori informazioni, consulta l'argomento relativo alla modifica degli indirizzi e-mail degli utenti.
3. Assicurati di migrare tutti i dati dalla casella di posta di Microsoft Exchange alla casella di posta di Amazon. WorkMail Per ulteriori informazioni, consulta Migrazione ad Amazon WorkMail.
4. Dopo la migrazione di tutti i dati, disabilita la cassetta postale dell'utente su Microsoft Exchange. Quindi, crea un utente di posta (o utente abilitato alla posta) con l'indirizzo SMTP esterno indirizzato ad Amazon. WorkMail A tale scopo, utilizza i seguenti comandi in Exchange Management Shell:

> **Important**
>
> I seguenti passaggi cancellano il contenuto della cassetta postale. Assicurati che i tuoi dati siano stati migrati su Amazon WorkMail prima di tentare di abilitare il routing delle e-mail. Alcuni client di posta non passano facilmente ad Amazon WorkMail quando esegui questo comando. Per ulteriori informazioni, consulta Configurazione del client delle e-mail.

```
$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
```

Nei comandi precedenti, *orgname* rappresenta il nome della tua WorkMail organizzazione Amazon. Per ulteriori informazioni, vedere Disabilitazione delle cassette postali e Abilitazione degli utenti di posta in Microsoft. TechNet

5. Invia un'e-mail di prova all'utente (nell'esempio precedente,**workmailuser@yourdomain.com**). Se il routing delle e-mail è stato abilitato correttamente, l'utente dovrebbe essere in grado di accedere alla propria WorkMail casella di posta Amazon e ricevere l'e-mail.

> **Note**
>
> Microsoft Exchange rimane impostato come server principale per le e-mail in entrata per il tempo che si desidera per disporre dell'interoperabilità tra i due ambienti. Per garantire l'interoperabilità con Microsoft Exchange, i record DNS non devono essere aggiornati in modo da indirizzare ad Amazon WorkMail solo in un secondo momento.

Configurazione successiva all'installazione

I passaggi precedenti spostano la cassetta postale di un utente da Microsoft Exchange Server ad Amazon WorkMail, mantenendo l'utente in Microsoft Exchange come contatto. Poiché l'utente migrato è ora un utente di posta esterno, Microsoft Exchange Server impone ulteriori vincoli. Potrebbero esserci anche requisiti di configurazione aggiuntivi per completare la migrazione.

- L'utente potrebbe non essere in grado di inviare e-mail ai gruppi di default. Per abilitare questa funzionalità, è necessario aggiungere l'utente a un elenco di mittenti sicuri per tutti i gruppi. Per ulteriori informazioni, vedi Gestione delle consegne in Microsoft TechNet.
- L'utente potrebbe non essere in grado di prenotare risorse. Per abilitare questa funzionalità, è necessario impostare tutte le risorse a cui l'utente deve accedere. `ProcessExternalMeetingMessages` Per ulteriori informazioni, vedere Set-CalendarProcessing on Microsoft TechNet.

Configurazione del client delle e-mail

Alcuni client di posta non passano facilmente ad Amazon WorkMail. Questi client richiedono all'utente di eseguire passaggi di configurazione aggiuntivi. Diversi client di posta richiedono l'esecuzione di diverse azioni.

- Microsoft Outlook su Windows: richiede il riavvio di Outlook. All'avvio, è necessario scegliere se continuare a utilizzare la casella postale precedente oppure utilizzarne una temporanea. Scegli l'opzione casella di posta temporanea. Quindi, riconfigurare la cassetta postale di Microsoft Exchange.
- Microsoft Outlook su macOS: al riavvio di Outlook, verrà visualizzato il seguente messaggio: Outlook è stato reindirizzato al server .awsapps.com. ***orgname*** Vuoi che questo server configuri le tue impostazioni? Accetta il suggerimento.
- Mail su iOS: l'app di posta smette di ricevere e-mail e genera un errore di impossibilità di ricevere la posta. Ricreare e riconfigurare la cassetta postale di Microsoft Exchange.

Disattivazione della modalità di interoperabilità e disattivazione del server di posta

Dopo aver configurato le caselle di posta di Microsoft Exchange per Amazon WorkMail, puoi disabilitare la modalità di interoperabilità. Se non hai migrato alcun utente o record, la disabilitazione della modalità di interoperabilità non influisce su nessuna delle tue configurazioni.

> **Warning**
>
> Prima di disabilitare la modalità di interoperabilità, assicuratevi di aver completato tutti i passaggi richiesti. In caso contrario, le e-mail potrebbero non essere inviate o potrebbero verificarsi comportamenti indesiderati. Se la migrazione non è stata completata, la disabilitazione dell'interoperabilità può provocare interruzioni all'interno della propria organizzazione. Questa operazione non può essere annullata.

Per disabilitare il supporto della modalità di interoperabilità

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli l'organizzazione per cui desideri disabilitare la modalità di interoperabilità.
3. In Impostazioni dell'organizzazione, scegli Disabilita la modalità di interoperabilità.
4. Nella finestra di dialogo Disabilita la modalità di interoperabilità, inserisci il nome dell'organizzazione e scegli Disabilita la modalità di interoperabilità.

Dopo aver disabilitato il supporto all'interoperabilità, gli utenti e i gruppi che non sono abilitati per Amazon WorkMail vengono rimossi dalla rubrica. Puoi comunque abilitare qualsiasi utente o gruppo mancante utilizzando la WorkMail console Amazon e questi verranno aggiunti alla rubrica. Le risorse di Microsoft Exchange non possono essere abilitate e non vengono visualizzate nella rubrica finché non completi il passaggio seguente.

- Crea risorse in Amazon WorkMail: puoi creare risorse in Amazon WorkMail e quindi configurare delegati e opzioni di prenotazione per queste risorse. Per ulteriori informazioni, consulta l'argomento relativo all'utilizzo delle risorse.
- Crea un record AutoDiscover DNS: configura un record AutoDiscover DNS per tutti i domini di posta dell'organizzazione. Ciò consente agli utenti di connettersi alle proprie WorkMail caselle di posta Amazon dai propri client Microsoft Outlook e mobili. Per ulteriori informazioni, consulta Utilizzare AutoDiscover per configurare gli endpoint.
- Trasferisci il tuo record MX DNS ad Amazon WorkMail: per recapitare tutte le e-mail in arrivo ad Amazon WorkMail, devi trasferire il tuo record MX DNS ad Amazon. WorkMail Le modifiche ai record DNS possono richiedere fino a 72 ore per propagarsi su tutti i server DNS.
- Disattiva il tuo server di posta: dopo aver verificato che tutte le e-mail vengano indirizzate direttamente ad Amazon WorkMail, puoi disattivare il server di posta se non intendi utilizzarlo in futuro.

Risoluzione dei problemi

Di seguito sono elencate le soluzioni agli errori di WorkMail interoperabilità e migrazione di Amazon più comuni.

L'URL di Exchange Web Services (EWS) non è valido o non è raggiungibile: verifica di avere l'URL EWS corretto. Per ulteriori informazioni, consulta Configurare le impostazioni di disponibilità su Amazon WorkMail.

Errore di connessione durante la convalida EWS: si tratta di un errore generale che può essere causato da:

- Nessuna connessione Internet in Microsoft Exchange.
- Il firewall non è configurato per consentire l'accesso da Internet. Verifica che la porta 443 (la porta predefinita per le richieste HTTPS) sia aperta.

Se hai confermato la connessione Internet e le impostazioni del firewall, ma l'errore persiste, contatta AWS Support.

Nome utente e password non validi durante la configurazione dell'interoperabilità di Microsoft Exchange: si tratta di un errore generale che può essere causato da:

- Il nome utente non è nella formato previsto. Utilizza lo schema seguente:

```
DOMAIN\username
```

- Il server di Microsoft Exchange non è configurato per l'autenticazione di base per EWS. Per ulteriori informazioni consulta l'argomento relativo a Virtual Directories: Exchange 2013 sul sito Microsoft MVP Award Program Blog.

L'utente riceve e-mail con allegato winmail.dat: ciò può accadere quando un'e-mail S/MIME crittografata viene inviata da Exchange ad Amazon WorkMail e ricevuta in Outlook 2016 per Mac o un client IMAP. La soluzione consiste nell'eseguire il seguente comando in Exchange Management Shell.

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

Se i punti sopraccitati sono stati confermati, ma l'errore persiste, contatta AWS Support.

WorkMail Quote Amazon

Amazon WorkMail può essere utilizzato sia dai clienti aziendali che dai proprietari di piccole imprese. Anche se supportiamo la maggior parte dei casi d'uso senza necessità di configurare modifiche delle quote, proteggiamo anche i nostri utenti e Internet dagli abusi del prodotto. Pertanto, alcuni clienti potrebbero incorrere nelle quote che abbiamo impostato. Questa sezione descrive questi quote e come modificarle.

Alcuni valori di quota possono essere modificati e altri sono quote rigide che non possono essere modificate. Per ulteriori informazioni sulla richiesta di un aumento delle quote, consultaQuote del servizio AWS nella Riferimenti generali di Amazon Web Services.

WorkMail Organizzazione Amazon e quote di utenti

Puoi aggiungere fino a 25 utenti alla tua WorkMail organizzazione Amazon per una prova gratuita di 30 giorni. Al termine di questo periodo, ti verranno addebitati i costi per tutti gli utenti attivi, a meno che non li rimuovi o chiudi il tuo WorkMail account Amazon.

Quando si valutano queste quote vengono considerati tutti i messaggi inviati ad altri utenti. Questi includono e-mail, richieste di riunioni, risposte di riunioni, richieste di attività e messaggi che vengono inoltrati o reindirizzati automaticamente come risultato di una regola.

> **Note**
>
> Quando richiedi un aumento della quota per un'organizzazione specifica, devi includere il nome dell'organizzazione nella richiesta.

Risorsa	Quota predefinita	Limite superiore per le richieste di modifica
WorkMail Organizzazioni Amazon per AWS account	100	Può essere aumentato in base al tipo di directory dell'orga nizzazione. È possibile visualizzare le AWS Directory Service quote e richiedere aumenti dalla AWS Directory Service console. Per ulteriori informazioni, consulta la sezione Service quotas nella Riferimenti generali di AWS.
Utenti per WorkMail organizza zione Amazon	1.000	Può essere aumentato a seconda del tipo di directory dell'organizzazione, come segue: • Amazon WorkMail directory: fino a 10 milioni di utenti • Simple AD o AD Connector , grandi dimensioni: fino a 5.000 utenti* • Simple AD o AD Connector , piccole dimensioni: fino a 500 utenti* • Microsoft AD, ospitato da AWS Directory Service: fino a 10 milioni di utenti

Risorsa	Quota predefinita	Limite superiore per le richieste di modifica
		a seconda della configura zione e della configurazione, * Se si sta usando Simple AD o AD Connector, consultar e l'articolo relativo a AWS Directory Service per ulteriori informazioni.
Utenti con periodo di prova gratuito	Fino a 25 utenti nei primi 30 giorni	Il periodo di prova gratuito è applicabile solo per i primi 25 utenti in qualsiasi organizza zione. Gli utenti aggiuntivi non sono inclusi nell'offerta di prova gratuita.
Destinatari indirizzati per AWS account al giorno	100.000 destinatari esterni all'organizzazione, senza alcuna quota rigida fissata per i destinatari interni all'organ izzazione.	Non vi sono limiti superiori. Tuttavia, Amazon WorkMail è un servizio di posta elettroni ca aziendale e non è destinato a essere utilizzato per servizi di posta elettronica di massa. Per i servizi di posta elettroni ca inviata in blocco, consultar e Amazon SES o Amazon Pinpoint.
Destinatari indirizzati per AWS account al giorno utilizzando uno dei domini di prova	200 destinatari, indipende ntemente dalla destinazione	Il dominio di posta di prova non è destinato all'uso a lungo termine. Ti consigliamo di aggiungere il tuo dominio e di utilizzarlo come dominio predefinito.

Le quote sui gruppi sono impostate dalla directory sottostante.

WorkMail organizzazione: impostazione delle quote

Risorsa	Quota predefinita
Numero di domini per organizzazione Amazon WorkMail	1.000 Questa è una quota rigida e non può essere modificata.
Numero di modelli mittente nelle regole del flusso di posta per ciascuna regola	250 Questa è una quota rigida e non può essere modificata.
Numero di modelli mittente nelle regole del flusso di posta per ciascuna organizzazione	1.000 Questa è una quota rigida e non può essere modificata.

Quote per utente

Quando si valutano queste quote vengono considerati tutti i messaggi inviati ad altri utenti. Questi includono e-mail, richieste di riunioni, risposte di riunioni, richieste di attività e messaggi che vengono inoltrati o reindirizzati automaticamente come risultato di una regola.

Risorsa	Quota predefinita	Quota massima per le richieste di modifica
Dimensione massima della mailbox	50 GB Questa è una quota rigida e non può essere modificata.	Non applicabile
Numero massimo di alias per ciascun utente.	100 Questa è una quota rigida e non può essere modificata.	Non applicabile

Risorsa	Quota predefinita	Quota massima per le richieste di modifica
Destinatari indirizzati per ciascun utente al giorno che utilizzano il dominio di proprietà	10.000 destinatari esterni all'organizzazione, senza alcuna quota rigida fissata per i destinatari interni all'organ izzazione.	Non vi sono limiti superiori. Tuttavia, Amazon WorkMail è un servizio di posta elettroni ca aziendale e non è destinato a essere utilizzato per servizi di posta elettronica di massa. Per i servizi di posta elettroni ca inviata in blocco, consultar e Amazon SES o Amazon Pinpoint.

Quote dei messaggi

Quando si valutano queste quote vengono considerati tutti i messaggi inviati ad altri utenti. Questi includono e-mail, richieste di riunioni, risposte di riunioni, richieste di attività e messaggi che vengono inoltrati o reindirizzati automaticamente come risultato di una regola.

Risorsa	Quota predefinita
Dimensioni massime dei messaggi in arrivo	29 MB di dati non codificati. I messaggi vengono ricevuti in formato MIME. La dimensione massima del messaggio MIME in arrivo è 40 MB. Questa è una quota fissa e non può essere modificata.
Dimensioni massime dei messaggi in uscita	29 MB di dati non codificati. I messaggi vengono inviati in formato MIME. La dimensione massima del messaggio MIME in uscita è 40 MB.

Risorsa	Quota predefinita
	Questa è una quota fissa e non può essere modificata.
Numero massimo di destinatari per messaggio	500 Questa è una quota rigida e non può essere modificata.
Numero massimo di allegati per messaggio	500 Questa è una quota fissa e non può essere modificata.

Utilizzo delle organizzazioni

In Amazon WorkMail, la tua organizzazione rappresenta gli utenti della tua azienda. Nella WorkMail console Amazon, viene visualizzato un elenco delle organizzazioni disponibili. Se non ne hai nessuna disponibile, devi creare un'organizzazione per poter utilizzare Amazon WorkMail.

Argomenti

Creazione di un'organizzazione

Per utilizzare Amazon WorkMail, devi prima creare un'organizzazione. Un AWS account può avere più WorkMail organizzazioni Amazon. Quando crei un'organizzazione, selezioni anche un dominio per l'organizzazione e configuri l'elenco degli utenti e le impostazioni di crittografia.

Puoi creare una nuova directory utente o integrare Amazon WorkMail con una directory esistente. Puoi usare Amazon WorkMail con Microsoft Active Directory, AWS Managed Active Directory o Simple AD locali. Grazie all'integrazione con la tua directory locale, puoi utilizzare gli utenti e i gruppi esistenti in Amazon WorkMail e gli utenti possono accedere con le loro credenziali esistenti. Se utilizzi una directory locale, devi prima configurare un AD Connector in AWS Directory Service. AD Connector sincronizza utenti e gruppi con la WorkMail rubrica di Amazon ed esegue le richieste di autenticazione degli utenti. Per ulteriori informazioni, consulta Active Directory Connector nella Guida all'AWS Directory Service amministrazione.

Hai anche la possibilità di selezionare uno AWS KMS key che Amazon WorkMail utilizza per crittografare il contenuto della casella di posta. Puoi selezionare la chiave master AWS gestita predefinita per Amazon WorkMail o utilizzare una chiave KMS esistente in AWS Key Management Service (AWS KMS). Per informazioni sulla creazione di una nuova chiave KMS, consulta Creating keys nella AWS Key Management Service Developer Guide. Se hai effettuato l'accesso come utente

AWS Identity and Access Management (IAM), diventa amministratore chiave della chiave KMS. Per ulteriori informazioni, consulta Abilitazione e disattivazione delle chiavi nella Guida per gli AWS Key Management Service sviluppatori.

Considerazioni

Quando crei un' WorkMail organizzazione Amazon, ricorda quanto segue:

- Amazon attualmente WorkMail non supporta i servizi Microsoft Active Directory gestiti che condividi con più account.
- Se disponi di un Active Directory locale con Microsoft Exchange e un AD Connector, ti consigliamo di configurare le impostazioni di interoperabilità per la tua organizzazione. Ciò consente di ridurre al minimo le interruzioni per gli utenti durante la migrazione delle cassette postali su Amazon o l'utilizzo di Amazon WorkMail WorkMail per un sottoinsieme delle caselle di posta aziendali. Per ulteriori informazioni, consulta Interoperabilità tra Amazon e WorkMail Microsoft Exchange.
- Se selezioni l'opzione Dominio di prova gratuito, puoi iniziare a utilizzare la tua WorkMail organizzazione Amazon con il dominio di prova fornito. Il dominio di test utilizza questo formato: *example* .awsapps.com. Puoi utilizzare il dominio di posta di prova con Amazon WorkMail e altri AWS servizi supportati purché mantenga utenti abilitati nella tua WorkMail organizzazione Amazon. Tuttavia, non puoi utilizzare il dominio di prova per altri scopi. Il dominio di prova potrebbe diventare disponibile per la registrazione e l'uso da parte di altri clienti se la tua WorkMail organizzazione Amazon non mantiene almeno un utente abilitato.
- Amazon WorkMail non supporta le directory multiregionali.

Argomenti

- Creazione di un'organizzazione
- Visualizzazione dei dettagli di un'organizzazione
- Integrazione di una directory WorkSpaces
- Stati e descrizioni delle organizzazioni

Creazione di un'organizzazione

Crea una nuova organizzazione nella WorkMail console Amazon.

Per creare un'organizzazione

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nella barra di navigazione, seleziona Organizzazione.

   Viene visualizzata la pagina Organizzazioni in cui sono visualizzate le organizzazioni, se presenti.
3. Scegli Crea organizzazione.
4. In Dominio e-mail, seleziona il dominio da utilizzare per gli indirizzi e-mail della tua organizzazione:

   - Dominio Route 53 esistente: seleziona un dominio esistente da gestire con una zona ospitata Amazon Route 53 (Route 53).
   - Nuovo dominio Route 53: registra un nuovo nome di dominio Route 53 da utilizzare con Amazon WorkMail.
   - Dominio esterno: inserisci un dominio esistente che gestisci con un provider DNS (Domain Name System) esterno.
   - Dominio di prova gratuito: utilizza un dominio di prova gratuito fornito da Amazon WorkMail. Puoi esplorare Amazon WorkMail utilizzando un dominio di prova e aggiungere un dominio alla tua organizzazione in un secondo momento.
5. (Facoltativo) Se il tuo dominio è gestito tramite Amazon Route 53, per la zona ospitata Route 53, seleziona il tuo dominio Route 53.
6. Per Alias, inserisci un alias univoco per la tua organizzazione.
7. Scegliete Impostazioni avanzate e, per Elenco utenti, selezionate una delle seguenti opzioni:

   - Crea una nuova WorkMail directory Amazon: crea una nuova directory per aggiungere e gestire i tuoi utenti.
   - Usa la directory esistente: utilizza una directory esistente per gestire gli utenti, ad esempio Microsoft Active Directory, AWS Managed Active Directory o Simple AD in locale.
8. Per la crittografia, seleziona una delle seguenti opzioni:

- Usa una chiave WorkMail gestita da Amazon: crea una nuova chiave di crittografia nel tuo account.
- Usa una chiave KMS esistente: utilizza una chiave KMS esistente in cui hai già creato. AWS KMS

9. Scegli Crea organizzazione.

Se utilizzi un dominio esterno, verificalo aggiungendo i record di testo (TXT) e mail exchanger (MX) appropriati al tuo servizio DNS. I record TXT consentono di inserire note sul servizio DNS. I record MX specificano il server di posta in arrivo.

Assicurati di impostare il dominio come predefinito per la tua organizzazione. Per ulteriori informazioni, consultare Verifica dei domini e Selezione del dominio predefinito.

Quando la tua organizzazione è attiva, puoi aggiungere utenti e configurare i loro client di posta elettronica. Per ulteriori informazioni, consulta Aggiunta di un utente Configurazione dei client di posta elettronica per Amazon WorkMail.

Visualizzazione dei dettagli di un'organizzazione

Ciascuna delle tue WorkMail organizzazioni Amazon può visualizzare una pagina dei dettagli dell'organizzazione. La pagina mostra informazioni sulla loro organizzazione, incluse quelle IDs che puoi utilizzare con AWS Command Line Interface. I messaggi sulla pagina possono anche mostrarti tutti i passaggi necessari per completare la configurazione e l'organizzazione, ad esempio un dominio non verificato o la mancanza di utenti. I messaggi forniscono anche il primo passaggio da seguire per configurare un determinato client di posta elettronica.

Per visualizzare i dettagli dell'organizzazione

1. Nella barra di navigazione, scegli Organizzazione.

   Viene visualizzata la pagina Organizzazioni in cui sono visualizzate le organizzazioni.
2. Scegli l'organizzazione che desideri visualizzare.

Integrazione di una directory WorkSpaces

Per usare Amazon WorkMail con WorkSpaces, crea una directory compatibile utilizzando i passaggi seguenti.

Per aggiungere una WorkSpaces directory compatibile

1. Crea una directory compatibile utilizzando WorkSpaces. Per WorkSpaces istruzioni, consulta la sezione Introduzione ad Amazon WorkSpaces Quick Setup nella Amazon WorkSpaces Administration Guide.
2. Nella WorkMail console Amazon, crea la tua WorkMail organizzazione Amazon e scegli di utilizzare per essa la directory esistente. Per ulteriori informazioni, consulta Creazione di un'organizzazione.

Stati e descrizioni delle organizzazioni

Dopo la creazione, l'organizzazione può avere uno dei seguenti stati.

Stato	Descrizione
Active (Attivo)	L'organizzazione è integra e pronta per essere utilizzata.
Creating (Creazione in corso)	Un flusso di lavoro è in esecuzione per creare l'organizzazione.
Failed (Non riuscito)	Non è possibile creare l'organizzazione.
Impaired (Insufficiente)	L'organizzazione non funziona correttamente o è stato rilevato un problema.
Inattivo	L'organizzazione non è attiva.
Requested (Richiesta)	La richiesta di creazione dell'organizzazione è in coda e in attesa di essere creata.
Validating (Convalida in corso)	Tutte le impostazioni per l'organizzazione sono in fase di verifica dello stato di integrità.

Eliminazione di un'organizzazione

Se non desideri più utilizzare Amazon WorkMail per l'e-mail della tua organizzazione, puoi eliminare la tua organizzazione da Amazon WorkMail.

> **Note**
>
> Questa operazione non può essere annullata. Non sarai in grado di recuperare i dati della tua casella di posta dopo l'eliminazione di un'organizzazione.

Per eliminare un'organizzazione

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nella schermata Organizzazioni, nell'elenco delle organizzazioni, seleziona l'organizzazione da eliminare e scegli Elimina.
3. Per Elimina organizzazione, scegli se eliminare o mantenere l'elenco utenti esistente, quindi inserisci il nome dell'organizzazione.
4. Scegli Elimina organizzazione.

> **Note**
>
> Se non hai fornito la tua directory per Amazon WorkMail, ne creeremo una per te. Se conservi questa directory esistente quando elimini l'organizzazione, ti verrà addebitato il costo WorkMail, WorkDocs a meno che non venga utilizzata da Amazon o WorkSpaces. Per informazioni sui prezzi consulta l'argomento relativo ai prezzi per altri tipi di directory.
> Per eliminare la directory, non è possibile abilitare nessun'altra AWS applicazione. Per ulteriori informazioni, vedere Eliminazione di una directory Simple AD o Eliminazione di una directory AD Connector nella Guida all'AWS Directory Service amministrazione.

Potresti ricevere un messaggio di errore relativo al set di regole di Amazon Simple Email Service (Amazon SES) non valido quando tenti di eliminare un'organizzazione. Se ricevi questo errore, modifica la regola Amazon SES nella console Amazon SES e rimuovi il set di regole non valido. La regola che modifichi deve avere WorkMail l'ID della tua organizzazione Amazon nel nome della

regola. Per ulteriori informazioni sulla modifica delle regole di Amazon SES, consulta Creazione di regole di ricezione nella Amazon Simple Email Service Developer Guide.

Se hai bisogno di capire quale set di regole non è valido, salva prima la regola. Viene visualizzato un messaggio di errore per il set di regole.

Ricerca di un indirizzo e-mail

Puoi scoprire se un indirizzo e-mail viene utilizzato nella tua organizzazione per utente, risorsa o gruppo.

Per trovare un indirizzo e-mail

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome di un'organizzazione.
3. Nella pagina Organizzazione, scegli Trova indirizzo email.
4. Selezionare Search (Cerca).

Lavorare con le impostazioni dell'organizzazione

Le seguenti sezioni spiegano come utilizzare le impostazioni disponibili per le WorkMail organizzazioni Amazon. Le impostazioni scelte verranno applicate all'intera organizzazione.

Argomenti

- Abilitazione della migrazione delle caselle di posta
- Attivazione del journaling
- Abilitare l'interoperabilità
- Abilitazione dei gateway SMTP
- Gestione dei flussi di e-mail
- Applicare le policy DMARC alla posta in entrata

Abilitazione della migrazione delle caselle di posta

Abilita la migrazione delle caselle di posta quando desideri trasferire le cassette postali da un'origine, come Microsoft Exchange o G Suite Basic, ad Amazon. WorkMail Abiliti la migrazione come parte di un processo di migrazione più ampio. Per ulteriori informazioni, incluse le istruzioni, consulta Migrazione ad Amazon WorkMail la sezione Guida introduttiva di questa guida.

Attivazione del journaling

Si abilita il journaling per registrare le comunicazioni via e-mail. Quando si utilizza il journaling, in genere si utilizzano strumenti di eDiscovery e archiviazione integrati di terze parti. Il journaling aiuta a garantire il rispetto delle normative di conformità per l'archiviazione dei dati, la protezione della privacy e la protezione delle informazioni.

Per ulteriori informazioni, incluse le istruzioni, consulta Usare l'e-mail journaling con Amazon WorkMail la sezione Guida introduttiva di questa guida.

Abilitare l'interoperabilità

L'interoperabilità consente di migrare da Microsoft Exchange e di utilizzare Amazon WorkMail come sottoinsieme delle caselle di posta aziendali. Per ulteriori informazioni, incluse le istruzioni, consulta la sezione Guida introduttiva di Configurare le impostazioni di disponibilità su Amazon WorkMail questa guida.

Abilitazione dei gateway SMTP

È possibile abilitare i gateway SMTP (Simple Mail Transfer Protocol) per l'utilizzo con le regole del flusso di posta elettronica in uscita. Le regole del flusso di posta elettronica in uscita ti consentono di instradare i messaggi e-mail inviati dalla tua WorkMail organizzazione Amazon tramite un gateway SMTP. Per ulteriori informazioni, consulta Operazioni delle regole di posta in uscita.

> **Note**
>
> I gateway SMTP configurati per le regole del flusso di posta elettronica in uscita devono supportare Transport Layer Security (TLS) v1.2 utilizzando certificati delle principali autorità di certificazione. Solo l'autenticazione di base è supportata.

Per configurare un gateway SMTP

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome di un'organizzazione.
3. Nel riquadro di navigazione selezionare Organization settings (Impostazioni organizzazione).

   Viene visualizzata la pagina delle impostazioni dell'organizzazione con una serie di schede.
4. Scegli la scheda Gateway SMTP, quindi scegli Crea gateway.
5. Immetti i seguenti dati:

   - Nome del gateway: inserisci un nome univoco.
   - Indirizzo gateway: immettere il nome host o l'indirizzo IP del gateway.
   - Numero di porta: immettere il numero di porta del gateway.
   - Nome utente: immettere un nome utente.
   - Password: inserisci una password sicura.
6. Scegli Create (Crea).

   Il gateway SMTP è disponibile per l'uso con le regole del flusso di posta in uscita.

Quando si configura un gateway SMTP da utilizzare con una regola del flusso di posta elettronica in uscita, i messaggi in uscita tentano di corrispondere alla regola con un gateway SMTP. I messaggi che corrispondono alla regola vengono indirizzati al gateway SMTP corrispondente, che gestisce quindi il resto del recapito delle e-mail.

Se Amazon non WorkMail è in grado di raggiungere il gateway SMTP, il sistema invia il messaggio e-mail al mittente. In tal caso, segui i passaggi precedenti per correggere le impostazioni del gateway.

Gestione dei flussi di e-mail

Per facilitare la gestione della posta elettronica, puoi configurare le regole del flusso di posta elettronica. Le regole del flusso di posta elettronica possono eseguire una o più azioni sui messaggi

di posta elettronica in base ai relativi indirizzi o domini. Puoi utilizzare le regole del flusso di posta elettronica sugli indirizzi e-mail o sui domini di mittenti e destinatari.

Quando si crea una regola del flusso di posta elettronica, si specifica un'azione della regola che si applica a un'e-mail quando viene rispettato uno schema di regole specificato.

Argomenti

Operazioni delle regole di posta in entrata

Le regole del flusso di posta in entrata consentono di impedire che le e-mail inviate da mittenti indesiderati raggiungano le mailbox degli utenti. Le regole del flusso di posta elettronica in entrata, chiamate anche azioni delle regole, si applicano automaticamente a tutti i messaggi e-mail inviati a chiunque all'interno della tua WorkMail organizzazione Amazon. Questo è diverso dalle regole di posta elettronica per le singole cassette postali.

> **Note**
>
> Facoltativamente, puoi utilizzare regole con una AWS Lambda funzione per elaborare la posta elettronica in arrivo prima che venga recapitata alle caselle di posta degli utenti. Per ulteriori informazioni sull'utilizzo di Lambda con Amazon WorkMail, consulta. Configurazione AWS Lambda per Amazon WorkMail Per ulteriori informazioni su Lambda, consulta la Guida per gli sviluppatori di AWS Lambda .

Le regole del flusso di posta elettronica in entrata, chiamate anche azioni delle regole, si applicano automaticamente a tutti i messaggi e-mail inviati a chiunque all'interno dell' WorkMail organizzazione Amazon. Questo è diverso dalle regole di posta elettronica per le singole cassette postali.

Le seguenti operazioni di regole definiscono il modo in cui viene gestita la posta in entrata. Per ogni regola è necessario specificare i modelli mittente e destinatario insieme a una delle seguenti azioni.

Azione	Descrizione
Drop email (Rilascia e-mail)	Il messaggio e-mail viene ignorato. L'e-mail non è recapitata e la mancata consegna non è notificata al mittente.
Send bounce response (Invia risposta di mancato recapito)	Il messaggio di posta elettronica non viene recapitato e il mittente viene avvisato del mancato recapito in un messaggio di rimbalzo.
Deliver to junk folder (Invia alla cartella spam)	Il messaggio e-mail viene recapitato nelle cartelle spam o posta indesiderata degli utenti, anche se non è stato originariamente identific ato come spam dal sistema di rilevamento dello WorkMail spam di Amazon.
Predefinita	Il messaggio e-mail viene recapitato dopo essere stato controllato dal sistema di rilevamento WorkMail dello spam di Amazon. L'e-mail spam viene recapitata nella cartella spam. Tutti gli altri messaggi e-mail vengono recapitati nella posta in arrivo. Le altre regole del flusso di posta con un modello di mittente meno specifico vengono ignorate. Per aggiungere eccezioni alle regole del flusso di posta basate su dominio, configura re l'operazione Default (Predefinita) con un modello di mittente più specifico. Per ulteriori informazioni, consulta Modelli mittente e destinatario.

Azione	Descrizione
Never deliver to junk folder (Non inviare mai alla cartella spam)	Il messaggio e-mail viene sempre recapitat o nelle caselle di posta degli utenti, anche se viene identificato come spam dal sistema di rilevamento dello WorkMail spam di Amazon. **Important** Non usando il sistema di rilevamento spam predefinito si potrebbe esporre gli utenti a contenuti ad alto rischio da indirizzi specificati dall'utente.
Esegui AWS Lambda	Passa il messaggio e-mail a una funzione Lambda per l'elaborazione prima o durante la consegna alle caselle di posta degli utenti.

Note

Le e-mail in entrata vengono prima recapitate ad Amazon SES e poi ad Amazon WorkMail. Se Amazon SES blocca un messaggio e-mail in entrata, le azioni relative alle regole non verranno applicate. Ad esempio, Amazon SES blocca un messaggio e-mail quando viene rilevato un virus noto o a causa di regole di filtraggio IP esplicite. La specifica di un'operazione di regola, ad esempio Default (Predefinito), Deliver to junk folder (Invia alla cartella spam) o Never deliver to junk folder (Non inviare mai alla cartella spam) non ha effetto.

Operazioni delle regole di posta in uscita

Utilizzi le regole del flusso di posta elettronica in uscita per indirizzare i messaggi di posta elettronica tramite gateway SMTP o per impedire ai mittenti di inviare messaggi e-mail a destinatari specifici. Per ulteriori informazioni sui gateway SMTP, vedere. Abilitazione dei gateway SMTP

È inoltre possibile utilizzare le regole del flusso di posta elettronica in uscita per passare il messaggio e-mail a una AWS Lambda funzione per l'elaborazione dopo l'invio dell'e-mail. Per ulteriori informazioni su Lambda, consulta la Guida per gli sviluppatori di AWS Lambda .

Le seguenti operazioni di regole definiscono il modo in cui viene gestita la posta in uscita. Per ogni regola è necessario specificare i modelli mittente e destinatario insieme a una delle seguenti azioni.

Azione	Descrizione
Default	Il messaggio di posta elettronica viene inviato tramite il normale flusso.
Drop email (Rilascia e-mail)	Il messaggio e-mail viene eliminato. Non viene inviata e il mittente non viene informato.
Send bounce response (Invia risposta di mancato recapito)	Il messaggio di posta elettronica non viene inviato e al mittente viene notificato con un messaggio che l'amministratore ha bloccato il messaggio di posta elettronica.
Instradamento a gateway SMTP	Il messaggio e-mail viene inviato tramite un gateway SMTP configurato.
Esegui Lambda	Passa il messaggio e-mail a una funzione Lambda per l'elaborazione prima o durante l'invio del messaggio di posta elettronica.

Modelli mittente e destinatario

Una regola per il flusso di e-mail può essere applicata a un indirizzo e-mail specifico o a tutti gli indirizzi e-mail in un dominio specifico o a un set di domini. È possibile definire un modello per determinare gli indirizzi e-mail ai quali si applica una regola.

I modelli mittente e destinatario accettano uno dei seguenti formati:

- Un indirizzo e-mail corrisponde a un singolo indirizzo e-mail; ad esempio:

```
mailbox@example.com
```

- Un nome di dominio corrisponde a tutti gli indirizzi e-mail di quel dominio; ad esempio:

```
example.com
```

- Un dominio wildcard corrisponde a tutti gli indirizzi e-mail di quel dominio e di tutti i relativi sottodomini. Un carattere jolly appare solo all'inizio di un dominio, ad esempio:

```
*.example.com
```

- Una stella corrisponde a tutti gli indirizzi e-mail di qualsiasi dominio.

```
*
```

> **Note**
>
> Il simbolo + non è valido all'interno dei modelli mittente o destinatario.

Per una regola possono essere specificati più modelli. Per ulteriori informazioni, consultare Operazioni delle regole di posta in entrata e Operazioni delle regole di posta in uscita.

Le regole del flusso di posta elettronica in entrata vengono applicate se l'`From`intestazione `Sender` o in un messaggio di posta elettronica in entrata corrisponde a uno schema. Se presente, viene innanzi tutto creata la corrispondenza dell'indirizzo `Sender`. L'indirizzo `From` viene abbinato in assenza di un'intestazione `Sender` oppure se l'intestazione `Sender` non corrisponde ad alcuna regola. Se ci sono più destinatari per il messaggio di posta elettronica che corrispondono a regole diverse, ogni regola si applica ai destinatari corrispondenti.

Le regole del flusso di posta elettronica in uscita vengono applicate se il destinatario e l'`From`intestazione `Sender` o in un messaggio di posta elettronica in uscita corrispondono a uno schema. Se ci sono più destinatari per il messaggio di posta elettronica che corrispondono a regole diverse, ogni regola si applica ai destinatari corrispondenti.

Se più regole corrispondono, viene applicata l'operazione della regola più specifica. Un esempio è quando una regola per un indirizzo e-mail specifico ha priorità rispetto a una regola che si applica a un intero dominio. Se più regole hanno la stessa specificità, viene applicata l'operazione più restrittiva. Un esempio è quando un'operazione di eliminazione ha priorità rispetto a un'operazione

di mancato recapito (bounce). L'ordine di precedenza per le azioni è lo stesso ordine in cui sono elencate in Operazioni delle regole di posta in entrata e Operazioni delle regole di posta in uscita.

> **Note**
>
> Fare attenzione durante la creazione di regole con modelli mittente sovrapposti con le azioni Drop (E-mail eliminata) o Bounce (Mancato recapito). Un ordine di precedenza imprevisto potrebbe comportare il mancato recapito di molti messaggi di posta elettronica in entrata.

Creazione di regole del flusso di posta elettronica

Le regole del flusso di posta elettronica applicano le azioni delle regole ai messaggi e-mail in entrata e in uscita. Le azioni si applicano quando i messaggi corrispondono a uno schema specificato. Le nuove regole del flusso di posta elettronica hanno effetto immediato.

Per creare regole per il flusso di posta elettronica

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome di un'organizzazione.
3. Nel riquadro di navigazione selezionare Organization settings (Impostazioni organizzazione).

   Viene visualizzata la pagina delle impostazioni dell'organizzazione con una serie di schede. Da questa pagina è possibile creare regole in entrata o in uscita. I passaggi seguenti spiegano come creare entrambi i tipi.

   Per creare regole in entrata

   1. Scegli la scheda Regole in entrata, quindi scegli Crea.
   2. Nella casella Nome regola, inserisci un nome univoco.
   3. In Azione, apri l'elenco e seleziona un'azione. Ogni elemento dell'elenco contiene una descrizione e alcuni forniscono collegamenti per saperne di più.

> **Note**
>
> Se si sceglie l'azione Esegui Lambda, vengono visualizzati controlli aggiuntivi: per informazioni sull'utilizzo di tali controlli, vedere la sezione successiva,. Configurazione AWS Lambda per Amazon WorkMail

4. In Domini o indirizzi del mittente, inserisci i domini o gli indirizzi del mittente a cui desideri applicare la regola.
5. In Domini o indirizzi di destinazione, inserisci qualsiasi combinazione di domini di destinazione e indirizzi e-mail.
6. Scegli Create (Crea).

Per creare regole in uscita

1. Scegli la scheda Regole in uscita e scegli Crea.
2. Nella casella Nome regola, inserisci un nome univoco.
3. In Azione, apri l'elenco e seleziona un'azione. Ogni elemento dell'elenco contiene una descrizione e alcuni forniscono collegamenti per saperne di più.

> **Note**
>
> Se si sceglie l'azione Esegui Lambda, vengono visualizzati controlli aggiuntivi. Per informazioni sull'utilizzo di questi controlli, consulta la sezione successiva,Configurazione AWS Lambda per Amazon WorkMail.

4. In Domini o indirizzi del mittente, inserisci qualsiasi combinazione di domini mittente e indirizzi e-mail validi.
5. In Domini o indirizzi di destinazione, inserisci qualsiasi combinazione di domini di destinazione e indirizzi e-mail validi.
6. Scegli Create (Crea).

È possibile testare la nuova regola per il flusso di posta creata. Per ulteriori informazioni, consulta Testare una regola per il flusso di e-mail.

Modifica delle regole del flusso di posta elettronica

Puoi modificare le regole del flusso di posta elettronica ogni volta che devi modificare una o più azioni delle regole per i messaggi e-mail. I passaggi descritti in questa sezione si applicano ai messaggi di posta elettronica in entrata e in uscita.

Per modificare le regole del flusso di posta elettronica

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome di un'organizzazione.
3. Nel riquadro di navigazione selezionare Organization settings (Impostazioni organizzazione).

   Viene visualizzata la pagina delle impostazioni dell'organizzazione con una serie di schede.
4. Scegli le schede Regole in entrata o Regole in uscita.
5. Scegli il pulsante di opzione accanto alla regola che desideri modificare, quindi scegli Modifica.
6. Modifica l'azione o le azioni nella regola in base alle esigenze, quindi scegli Salva.

Configurazione AWS Lambda per Amazon WorkMail

Utilizza l'azione Esegui Lambda nelle regole del flusso di posta elettronica in entrata e in uscita per passare i messaggi e-mail che corrispondono alle regole a una AWS Lambda funzione di elaborazione.

Scegli tra le seguenti configurazioni per un'azione Esegui Lambda in Amazon. WorkMail

Configurazione Synchronous Run Lambda

> I messaggi di posta elettronica che corrispondono alla regola del flusso vengono passati a una funzione Lambda per l'elaborazione prima di essere inviati o recapitati. Utilizzate questa configurazione per modificare il contenuto delle e-mail. Puoi anche controllare il flusso di posta elettronica in entrata o in uscita per diversi casi d'uso. Ad esempio, una regola passata a una funzione Lambda può bloccare la consegna di messaggi e-mail sensibili, rimuovere allegati o aggiungere dichiarazioni di non responsabilità.

Configurazione Run Lambda asincrona

I messaggi di posta elettronica che corrispondono alla regola del flusso vengono passati a una funzione Lambda per l'elaborazione durante l'invio o la consegna. Questa configurazione non influisce sulla consegna delle e-mail e viene utilizzata per attività quali la raccolta di parametri relativi ai messaggi e-mail in entrata o in uscita.

Sia che si scelga una configurazione sincrona o asincrona, l'oggetto evento passato alla funzione Lambda contiene i metadati per l'evento e-mail in entrata o in uscita. È inoltre possibile utilizzare l'ID messaggio nei metadati per accedere all'intero contenuto del messaggio e-mail. Per ulteriori informazioni, consulta Recupero del contenuto del messaggio con AWS Lambda. Per ulteriori informazioni sugli eventi, consulta Dati degli eventi Lambda.

Per ulteriori informazioni sulle regole del flusso di posta in entrata e in uscita, consulta Gestione dei flussi di e-mail. Per ulteriori informazioni su Lambda, consulta la Guida per gli sviluppatori di AWS Lambda .

> **Note**
>
> Attualmente, le regole del flusso di posta elettronica Lambda fanno riferimento solo alle funzioni Lambda nella stessa regione AWS e Account AWS nell'organizzazione Amazon WorkMail da configurare.

Guida introduttiva AWS Lambda per Amazon WorkMail

Per iniziare AWS Lambda a usare Amazon WorkMail, ti consigliamo di distribuire la funzione WorkMail Hello World Lambda dal AWS Serverless Application Repository al tuo account. La funzione dispone di tutte le risorse necessarie e le autorizzazioni sono configurate per te. Per altri esempi, consulta il amazon-workmail-lambda-templatesrepository su. GitHub

Se scegli di creare la tua funzione Lambda, devi configurare le autorizzazioni utilizzando (). AWS Command Line Interface AWS CLI Nel seguente comando di esempio, effettuate le seguenti operazioni:

- Sostituisci `MY_FUNCTION_NAME` con il nome della tua funzione Lambda.
- `REGION`Sostituiscilo con la tua regione Amazon WorkMail AWS. Le WorkMail regioni Amazon disponibili includono `us-east-1` (Stati Uniti orientali (Virginia settentrionale)), `us-west-2` (Stati Uniti occidentali (Oregon)) e `eu-west-1` (Europa (Irlanda)).

- Sostituiscilo `AWS_ACCOUNT_ID` con il tuo ID a 12 cifre Account AWS .
- `WORKMAIL_ORGANIZATION_ID`Sostituiscilo con WorkMail l'ID della tua organizzazione Amazon. Puoi trovarlo sulla scheda della tua organizzazione nella pagina 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
```

Per ulteriori informazioni sull'utilizzo di AWS CLI, consulta la Guida AWS Command Line Interface per l'utente.

Configurazione delle regole Run Lambda sincrone

Per configurare una regola sincrona Esegui Lambda, crea una regola del flusso di posta elettronica con l'azione Esegui Lambda e seleziona la casella di controllo Esegui in modo sincrono. Per ulteriori informazioni sulla creazione di regole del flusso di e-mail, consulta Creazione di regole del flusso di posta elettronica.

Per completare la creazione della regola sincrona, aggiungi Lambda Amazon Resource Name (ARN) e configura le seguenti opzioni.

Operazione di fallback

L'azione WorkMail applicata da Amazon se la funzione Lambda non viene eseguita. Questa azione si applica anche a tutti i destinatari che vengono omessi dalla risposta Lambda se il flag AllRecipients non è impostato. L'azione Fallback non può essere un'altra azione Lambda.

Timeout regola (in minuti).

Il periodo di tempo durante il quale la funzione Lambda viene ritentata se Amazon WorkMail non riesce a richiamarla. Operazione di fallback viene applicata alla fine di questo periodo di tempo.

> **Note**
>
> Le regole Synchronous Run Lambda supportano solo ***** la condizione di destinazione.

Dati degli eventi Lambda

La funzione Lambda viene attivata utilizzando i seguenti dati di evento. La presentazione dei dati varia a seconda del linguaggio di programmazione utilizzato per la funzione Lambda.

```
{
    "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
}
```

Il JSON di evento include i seguenti dati.

summaryVersion

Il numero di versione per`LambdaEventData`. Si aggiorna solo quando apporti una modifica incompatibile con le versioni precedenti. `LambdaEventData`

envelope

La busta del messaggio di posta elettronica, che include i seguenti campi.

mailFrom

L'indirizzo Da, che di solito è l'indirizzo e-mail dell'utente che ha inviato il messaggio e-mail. Se l'utente ha inviato il messaggio come un altro utente o per conto di un altro utente, il campo mailFrom restituisce l'indirizzo e-mail dell'utente per conto del quale è stata inviata l'e-mail e non l'indirizzo e-mail del mittente effettivo.

recipients

L'elenco degli indirizzi e-mail dei destinatari. Amazon WorkMail non fa distinzione tra To, CC o BCC.

> **Note**
>
> Per le regole del flusso di posta elettronica in entrata, questo elenco include i destinatari in tutti i domini dell' WorkMailorganizzazione Amazon in cui crei la regola. La funzione Lambda viene richiamata separatamente per ogni conversazione SMTP dal mittente e il campo destinatari elenca i destinatari di quella conversazione SMTP. I destinatari con domini esterni non sono inclusi.

mittente

L'indirizzo e-mail dell'utente che ha inviato il messaggio e-mail per conto di un altro utente. Questo campo è impostato solo quando un messaggio e-mail viene inviato per conto di un altro utente.

subject

La riga dell'oggetto del messaggio e-mail. Viene troncata quando supera il limite di 256 caratteri.

messageId

Un ID univoco utilizzato per accedere all'intero contenuto del messaggio e-mail quando si utilizza l'SDK Amazon WorkMail Message Flow.

InvocationID

L'ID per una chiamata Lambda univoca. Questo ID rimane lo stesso quando una funzione Lambda viene chiamata più di una volta per la stessa. LambdaEventData Utilizzare per rilevare i tentativi ed evitare la duplicazione.

flowDirection

Indica la direzione del flusso di e-mail, INBOUND o OUTBOUND.

truncated

Si applica alla dimensione del payload e non alla lunghezza della riga dell'oggetto. Se `true`, la dimensione del payload supera il limite di 128 KB, per cui l'elenco dei destinatari viene troncato in modo da soddisfare il limite.

Schema di risposta Lambda Synchronous Run

Quando una regola del flusso e-mail con un'azione sincrona Esegui Lambda corrisponde a un messaggio e-mail in entrata o in uscita, Amazon WorkMail chiama la funzione Lambda configurata e attende la risposta prima di agire sul messaggio e-mail. La funzione Lambda restituisce una risposta secondo uno schema predefinito che elenca le azioni, i tipi di azione, i parametri applicabili e i destinatari a cui si applica l'azione.

L'esempio seguente mostra una risposta sincrona Run Lambda. Le risposte variano in base al linguaggio di programmazione utilizzato per la funzione Lambda.

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

La risposta JSON include i seguenti dati.

action

Operazione da intraprendere per i destinatari.

tipo

Tipo di operazione. I tipi di azione non vengono restituiti per le azioni Run Lambda asincrone.

I tipi di operazioni delle regole in entrata includono BOUNCE, DROP, DEFAULT, BYPASS_SPAM_CHECK e MOVE_TO_JUNK. Per ulteriori informazioni, consulta Operazioni delle regole di posta in entrata.

I tipi di operazioni delle regole in uscita includono BOUNCE, DROP e DEFAULT. Per ulteriori informazioni, consulta Operazioni delle regole di posta in uscita.

parametri

Parametri di operazione aggiuntivi. Supportato per il tipo di operazione BOUNCE come oggetto JSON con la chiave bounceMessage e la stringa del valore. Questo messaggio di mancato recapito (bounce) viene utilizzato per creare il messaggio e-mail di mancato recapito (bounce).

recipients

Elenco di indirizzi e-mail su cui deve essere intrapresa l'operazione. È possibile aggiungere nuovi destinatari alla risposta anche se non sono stati inclusi nell'elenco dei destinatari originali. Questo campo non è obbligatorio se allRecipients ha il valore true per un'operazione.

> **Note**
>
> Quando viene richiesta un'azione Lambda per la posta elettronica in entrata, è possibile aggiungere solo nuovi destinatari che provengono dalla propria organizzazione. I nuovi destinatari vengono aggiunti alla risposta come Ccn.

allRecipients

Se impostato su true, applica l'azione a tutti i destinatari che non sono soggetti a un'altra azione specifica nella risposta Lambda.

Limiti di azione Lambda di Synchronous Run

I seguenti limiti si applicano quando Amazon WorkMail richiama le funzioni Lambda per azioni sincrone Run Lambda:

- Le funzioni Lambda devono rispondere entro 15 secondi o essere trattate come chiamate non riuscite.

  > **Note**
  >
  > Il sistema riprova la chiamata per l'intervallo di timeout della regola specificato.

- Sono consentite risposte della funzione Lambda fino a 256 KB.
- Nella risposta sono consentite fino a 10 operazioni univoche. Le operazioni superiori a 10 sono soggette all'Operazione di fallback configurata.

- Sono consentiti fino a 500 destinatari per le funzioni Lambda in uscita.
- Il valore massimo per Timeout regola è 240 minuti. Se è configurato il valore minimo 0, non ci sono nuovi tentativi prima che Amazon WorkMail applichi l'azione di fallback.

Errori dell'azione Synchronous Run Lambda

Se Amazon non WorkMail riesce a richiamare la funzione Lambda a causa di un errore, di una risposta non valida o di un timeout Lambda, WorkMail Amazon ritenta la chiamata con un backoff esponenziale che riduce la velocità di elaborazione fino al completamento del periodo di timeout della regola. Quindi, l'Operazione di fallback viene applicata a tutti i destinatari del messaggio e-mail. Per ulteriori informazioni, consulta Configurazione delle regole Run Lambda sincrone.

Esempi di risposte Run Lambda sincrone

Gli esempi seguenti illustrano la struttura delle risposte Run Lambda sincrone comuni.

Example : rimozione dei destinatari specificati da un messaggio e-mail

L'esempio seguente dimostra la struttura di una risposta sincrona Run Lambda per rimuovere i destinatari da un messaggio di posta elettronica.

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

Example : mancato recapito (bounce) con un messaggio e-mail personalizzato

L'esempio seguente dimostra la struttura di una risposta sincrona Run Lambda per il rimbalzo con un messaggio e-mail personalizzato.

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

Example : aggiunta di destinatari a un messaggio e-mail

L'esempio seguente dimostra la struttura di una risposta sincrona Run Lambda per aggiungere destinatari al messaggio di posta elettronica. Questa operazione non aggiorna i campi A o Cc del messaggio e-mail.

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

```
}
```

Per altri esempi di codice da utilizzare durante la creazione di funzioni Lambda per le azioni Esegui Lambda, consulta i modelli di Amazon Lambda. WorkMail

Ulteriori informazioni sull'utilizzo di Lambda con Amazon WorkMail

Puoi anche accedere al contenuto completo del messaggio e-mail che attiva la funzione Lambda. Per ulteriori informazioni, consulta Recupero del contenuto del messaggio con AWS Lambda.

Recupero del contenuto del messaggio con AWS Lambda

Dopo aver configurato una AWS Lambda funzione per gestire i flussi di posta elettronica per Amazon WorkMail, puoi accedere al contenuto completo dei messaggi e-mail elaborati con Lambda. Per ulteriori informazioni su come iniziare a usare Lambda for Amazon WorkMail, consulta. Configurazione AWS Lambda per Amazon WorkMail

Per accedere al contenuto completo dei messaggi e-mail, utilizza l'`GetRawMessageContent`azione nell'API Amazon WorkMail Message Flow. L'ID del messaggio e-mail passato alla funzione Lambda al momento della chiamata invia una richiesta all'API. Quindi, l'API risponde con il contenuto MIME completo del messaggio e-mail. Per ulteriori informazioni, consulta Amazon WorkMail Message Flow nell'Amazon WorkMail API Reference.

L'esempio seguente mostra come una funzione Lambda che utilizza l'ambiente di runtime Python può recuperare il contenuto completo del messaggio.

> **Tip**
>
> Se inizi distribuendo la funzione Amazon WorkMail Hello World Lambda dal al tuo account, AWS Serverless Application Repository il sistema crea una funzione Lambda nel tuo account con tutte le risorse e le autorizzazioni necessarie. Puoi quindi aggiungere la tua logica di business alla funzione lambda in base al tuo caso d'uso.

```
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)
```

Per esempi più dettagliati di modi per analizzare il contenuto dei messaggi in transito, consulta il amazon-workmail-lambda-templatesrepository su. GitHub

> **Note**
>
> L'API Amazon WorkMail Message Flow viene utilizzata solo per accedere ai messaggi e-mail in transito. Puoi accedere ai messaggi solo entro 24 ore dall'invio o dalla ricezione. Per accedere in modo programmatico ai messaggi nella casella di posta di un utente, utilizza uno degli altri protocolli supportati da Amazon WorkMail, come IMAP o Exchange Web Services (EWS).

Aggiornamento del contenuto dei messaggi con AWS Lambda

Dopo aver configurato una AWS Lambda funzione sincrona per gestire i flussi di posta elettronica, puoi utilizzare l'`PutRawMessageContent`azione nell'API Amazon WorkMail Message Flow per aggiornare il contenuto dei messaggi e-mail in transito. Per ulteriori informazioni su come iniziare a usare le funzioni Lambda per Amazon WorkMail, consulta. Configurazione delle regole Run Lambda sincrone Per ulteriori informazioni sull'API, consulta PutRawMessageContent.

> **Note**
>
> L' PutRawMessageContent API richiede boto3 1.17.8 oppure puoi aggiungere un layer alla tua funzione Lambda. Per scaricare la versione boto3 corretta, consulta la pagina di avvio su. GitHub Per ulteriori informazioni sull'aggiunta di livelli, consulta Configurare una funzione per l'uso dei livelli.
> Ecco un esempio di livello:`"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`. In questo esempio, sostituiscilo `${AWS::Region}` con una regione aws appropriata, come us-east-1.

> **Tip**
>
> Se inizi distribuendo la funzione Amazon WorkMail Hello World Lambda da AWS Serverless Application Repository al tuo account, il sistema crea una funzione Lambda nel tuo account con le risorse e le autorizzazioni necessarie. Puoi quindi aggiungere la logica di business alla funzione lambda, in base ai tuoi casi d'uso.

Mentre procedi, ricorda quanto segue:

- Utilizza l' GetRawMessageContentAPI per recuperare il contenuto originale del messaggio. Per ulteriori informazioni, consulta Recupero del contenuto del messaggio con AWS Lambda.
- Una volta che hai il messaggio originale, modifica il contenuto MIME. Al termine, carica il messaggio in un bucket Amazon Simple Storage Service (Amazon S3) nel tuo account. Assicurati che il bucket S3 utilizzi lo Account AWS stesso delle tue WorkMail operazioni Amazon e che utilizzi la stessa regione AWS delle tue chiamate API.
- Affinché Amazon WorkMail elabori le richieste, il tuo bucket S3 deve avere la politica corretta per accedere all'oggetto S3. Per ulteriori informazioni, consulta Example S3 policy.
- Utilizza l' PutRawMessageContentAPI per inviare il contenuto aggiornato del messaggio ad Amazon WorkMail.

> **Note**
>
> L'`PutRawMessageContent`API garantisce che il contenuto MIME del messaggio aggiornato soddisfi gli standard RFC, nonché i criteri indicati nel RawMessageContenttipo di dati. Le e-mail in arrivo verso la tua WorkMail organizzazione Amazon non sempre soddisfano questi standard, quindi l'`PutRawMessageContent`API potrebbe rifiutarle. In questi casi, puoi consultare il messaggio di errore restituito per ulteriori informazioni su come risolvere eventuali problemi.

Example Esempio di politica S3

```
{
    "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/*"
                }
            }
        }
    ]
}
```

L'esempio seguente mostra come una funzione Lambda utilizzi il runtime Python per aggiornare l'oggetto di un messaggio di posta elettronica in transito.

```
    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)
```

Per altri esempi di modi per analizzare il contenuto dei messaggi in transito, consultate il repository su. amazon-workmail-lambda-templates GitHub

Gestione dell'accesso all'API Amazon WorkMail Message Flow

Utilizza le policy AWS Identity and Access Management (IAM) per gestire l'accesso all'API Amazon WorkMail Message Flow.

L'API Amazon WorkMail Message Flow funziona con un unico tipo di risorsa, un messaggio e-mail in transito. A ogni messaggio e-mail in transito è associato un Amazon Resource Name (ARN) univoco.

L'esempio seguente mostra la sintassi di un ARN associato a un messaggio e-mail in transito.

```
arn:aws:workmailmessageflow:region:account:message/organization/context/messageID
```

I campi modificabili nell'esempio precedente sono i seguenti:

- Regione: la regione AWS per la tua WorkMail organizzazione Amazon.
- Account: l' Account AWS ID della tua WorkMail organizzazione Amazon.
- Organizzazione: l'ID WorkMail della tua organizzazione Amazon.
- Contesto: indica se il messaggio è `incoming` diretto alla tua organizzazione o `outgoing` proviene da essa.

- ID messaggio: l'ID univoco del messaggio di posta elettronica che viene passato come input alla funzione Lambda.

L'esempio seguente include un IDs esempio di ARN associato a un messaggio di posta elettronica in arrivo in transito.

```
arn:aws:workmailmessageflow:us-east-1:111122223333:message/m-
n1pq2345678r901st2u3vx45x6789yza/incoming/d1234567-8e90-1f23-456g-hjk7lmnop8q9
```

Puoi utilizzarli ARNs come risorse nella `Resource` sezione delle politiche utente IAM per gestire l'accesso ai WorkMail messaggi Amazon in transito.

Esempi di politiche IAM per l'accesso al flusso di WorkMail messaggi di Amazon

La seguente policy di esempio concede a un'entità IAM l'accesso completo in lettura a tutti i messaggi in entrata e in uscita per ogni WorkMail organizzazione Amazon della tua azienda. Account AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

Se hai più organizzazioni al tuo interno Account AWS, puoi anche limitare l'accesso a una o più organizzazioni. Ciò è utile se determinate funzioni Lambda devono essere utilizzate solo per determinate organizzazioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
```

```
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/*",
            "Effect": "Allow"
        }
    ]
}
```

Puoi anche scegliere di concedere l'accesso ai messaggi a seconda che siano `incoming` nella tua organizzazione o `outgoing` da essa. Per eseguire questa operazione, utilizza il qualificatore `incoming` o `outgoing` nell'ARN.

La policy di esempio seguente concede l'accesso solo ai messaggi in entrata nella tua organizzazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/incoming/*",
            "Effect": "Allow"
        }
    ]
}
```

La seguente policy di esempio concede a un'entità IAM l'accesso completo in lettura e aggiornamento a tutti i messaggi in entrata e in uscita per ogni WorkMail organizzazione Amazon della tua azienda. Account AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent",
                "workmailmessageflow:PutRawMessageContent"
            ],
```

```
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

Testare una regola per il flusso di e-mail

Per verificare l'attuale configurazione della regola è possibile testare il modo in cui la configurazione si comporta rispetto a indirizzi e-mail specifici.

Per testare una regola per il flusso di e-mail

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione selezionare Organization settings (Impostazioni organizzazione), Inbound/Outbound rules (Regole in entrata/in uscita).
4. Accanto a Test configuration (Test della configurazione), immettere gli indirizzi e-mail completi del mittente e del destinatario da testare.
5. Scegli Test (Esegui test). Viene visualizzata l'operazione che verrà eseguita per l'indirizzo e-mail fornito.

Rimozione di una regola per il flusso di e-mail

Quando si rimuove una regola per il flusso di e-mail, le modifiche vengono applicate immediatamente.

Per rimuovere una regola per il flusso di e-mail

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione selezionare Organization settings (Impostazioni organizzazione), Inbound/Outbound rules (Regole in entrata/in uscita).
4. Selezionare la regola, quindi selezionare Remove (Rimuovi).
5. Alla richiesta di conferma selezionare Remove (Rimuovi).

Applicare le policy DMARC alla posta in entrata

I domini di posta elettronica utilizzano i record DNS (Domain Name System) per motivi di sicurezza. Proteggono gli utenti da attacchi comuni come lo spoofing o il phishing. I record DNS includono spesso i record DMARC (Domain-based Message Authentication, Reporting and Conformance), che vengono impostati dal proprietario del dominio che invia l'e-mail. I record DMARC includono politiche che specificano le azioni da intraprendere quando un'e-mail non supera un controllo DMARC. È possibile scegliere se applicare la policy DMARC sui messaggi inviati all'organizzazione.

Le nuove WorkMail organizzazioni Amazon hanno l'applicazione DMARC attivata per impostazione predefinita.

Per attivare l'applicazione DMARC

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione selezionare Organization settings (Impostazioni organizzazione). Viene visualizzata la pagina delle impostazioni dell'organizzazione con una serie di schede.
4. Scegli la scheda DMARC, quindi scegli Modifica.
5. Sposta il cursore di imposizione DMARC in posizione On.
6. Seleziona la casella di controllo accanto a Riconosco che l'attivazione dell'applicazione DMARC può comportare l'eliminazione o la messa in quarantena delle e-mail in entrata in base alla configurazione del dominio del mittente.
7. Scegli Save (Salva).

Per disattivare l'applicazione DMARC

- Segui i passaggi della sezione precedente, ma sposta il cursore di imposizione DMARC in posizione OFF.

Utilizzo della registrazione eventi e-mail per tenere traccia dell'applicazione DMARC

Attivando l'applicazione DMARC, è possibile che le e-mail in entrata vengano eliminate o contrassegnate come posta indesiderata, a seconda di come il mittente ha configurato il proprio dominio. Se un mittente configura erroneamente il proprio dominio di posta elettronica, gli utenti potrebbero smettere di ricevere le e-mail legittime. Per verificare la presenza di e-mail che non vengono recapitate ai tuoi utenti, puoi abilitare la registrazione degli eventi e-mail per la tua WorkMail organizzazione Amazon. Quindi, è possibile eseguire una query nei log di eventi di posta elettronica per i messaggi in entrata che vengono filtrati in base alle policy DMARC del mittente.

Prima di utilizzare la registrazione degli eventi e-mail per monitorare l'applicazione del DMARC, abilita la registrazione degli eventi e-mail nella console Amazon. WorkMail Per ottenere il massimo dai dati del log, lascia passare un po' di tempo durante la registrazione degli eventi e-mail. Per ulteriori informazioni e istruzioni, consulta the section called “Per disattivare la registrazione degli eventi e-mail”.

Per utilizzare la registrazione degli eventi di posta elettronica per tracciare l'applicazione DMARC

1. Nella console CloudWatch Insights, in Logs, scegli Insights.
2. Per Seleziona gruppi di log, seleziona il gruppo di log della tua WorkMail organizzazione Amazon. Ad esempio,/aws/workmail/events/organization-alias.
3. Seleziona un periodo di tempo per la query.
4. Esegui la seguente query: stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. Scegli Esegui query.

Puoi inoltre impostare parametri personalizzati per questi eventi. Per ulteriori informazioni, consulta Creazione di filtri di parametri.

Tagging di un'organizzazione

L'aggiunta di tag a una risorsa WorkMail dell'organizzazione Amazon ti consente di:

- Distinguere le organizzazioni nella AWS Billing and Cost Management console.
- Controlla l'accesso alle risorse WorkMail dell'organizzazione Amazon aggiungendole alle dichiarazioni sulla politica di autorizzazione `Resource` Element of AWS Identity and Access Management (IAM).

Per ulteriori informazioni sulle autorizzazioni a WorkMail livello di risorsa di Amazon, consulta. Risorse Per ulteriori informazioni sul controllo dell'accesso basato su tag, consulta Autorizzazione basata sui WorkMail tag Amazon.

WorkMail Gli amministratori di Amazon possono taggare le organizzazioni utilizzando la WorkMail console Amazon.

Per aggiungere tag a un' WorkMail organizzazione Amazon

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Scegliere Tags (Tag).
4. In Organization tags (Tag organizzazione), scegliere Add new tag (Aggiungi nuovo tag).
5. Per Chiave, inserisci un nome che identifichi il tag.
6. (Facoltativo) In Value (Valore), inserire un valore per il tag.
7. (Facoltativo) Ripetere le fasi da 4 a 6 per aggiungere altri tag all'organizzazione. Puoi aggiungere fino a 50 tag.
8. Scegliere Salva per salvare le modifiche.

Puoi visualizzare i tag della tua organizzazione nella WorkMail console Amazon.

Gli sviluppatori possono anche taggare le organizzazioni utilizzando l' AWS SDK o AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consulta i `UntagResource` comandi `TagResource`, `ListTagsForResource`, e in Amazon WorkMail API Reference o AWS CLI Command Reference.

Puoi rimuovere i tag da un'organizzazione in qualsiasi momento, utilizzando la WorkMail console Amazon.

Per rimuovere i tag da un' WorkMail organizzazione Amazon

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Scegliere Tags (Tag).
4. In Organization tags (Tag organizzazione, scegliere Remove (Rimuovi) accanto al tag da rimuovere.
5. Scegliere Submit (Invia) per salvare le modifiche.

Utilizzo delle regole di controllo degli accessi

Le regole di controllo degli accessi per Amazon WorkMail consentono agli amministratori di controllare in che modo agli utenti e ai ruoli di impersonificazione della propria organizzazione viene concesso l'accesso ad Amazon. WorkMail Ogni WorkMail organizzazione Amazon ha una regola di controllo degli accessi predefinita che concede l'accesso alla casella di posta elettronica a tutti gli utenti e ai ruoli di impersonificazione aggiunti all'organizzazione, indipendentemente dal protocollo di accesso o dall'indirizzo IP utilizzati. Gli amministratori possono modificare o sostituire la regola predefinita con una propria, aggiungere una nuova regola o eliminarla.

> **Warning**
>
> Se un amministratore elimina tutte le regole di controllo degli accessi per un'organizzazione, Amazon WorkMail blocca tutti gli accessi alle caselle di posta dell'organizzazione.

Gli amministratori possono applicare regole di controllo degli accessi che consentono o negano l'accesso in base ai criteri seguenti:

- Protocolli: il protocollo utilizzato per accedere alla casella di posta. Gli esempi includono Autodiscover, EWS, IMAP, SMTP ActiveSync, Outlook per Windows e Webmail.
- Indirizzi IP: gli intervalli IPv4 CIDR utilizzati per accedere alla casella di posta.
- WorkMail Utenti Amazon: gli utenti della tua organizzazione utilizzati per accedere alla casella di posta.
- Ruoli di impersonificazione: i ruoli di impersonificazione nell'organizzazione utilizzati per accedere alla casella di posta. Per ulteriori informazioni, consulta Gestione dei ruoli di impersonificazione.

Gli amministratori applicano le regole di controllo degli accessi oltre alle autorizzazioni delle cassette postali e delle cartelle dell'utente. Per ulteriori informazioni, consulta Utilizzo delle autorizzazioni della casella di posta Condivisione di cartelle e autorizzazioni per le cartelle nella Amazon WorkMail User Guide.

> **Note**
>
> - Quando si abilita l'accesso per Outlook per Windows, si consiglia di abilitare anche l'accesso per Autodiscover ed EWS.
> - Le regole di controllo degli accessi non si applicano all'accesso WorkMail tramite console Amazon o SDK. Utilizza invece ruoli o politiche AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per Amazon WorkMail.

Creazione di regole di controllo degli accessi

Crea nuove regole di controllo degli accessi dalla WorkMail console Amazon.

Per creare una nuova regola di controllo degli accessi

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.

3. Scegliere Access control rules (Regole di controllo accessi).
4. Scegli Crea regola.
5. Per Description (Descrizione), immettere una descrizione per la regola.
6. Per Effect (Effetto), scegliere Allow (Consenti) o Deny (Nega). Ciò consente o nega l'accesso in base alle condizioni selezionate nel passaggio seguente.
7. Perché Questa regola si applica alle richieste che... , seleziona le condizioni da applicare alla regola, ad esempio se includere o escludere protocolli, indirizzi IP o utenti specifici o ruoli di impersonificazione.
8. (Facoltativo) Se inserisci intervalli di indirizzi IP, utenti o ruoli di impersonificazione, scegli Aggiungi per aggiungerli alla regola.
9. Scegli Crea regola.

Modifica delle regole di controllo degli accessi

Modifica le regole di controllo degli accessi nuove e predefinite dalla WorkMail console Amazon.

Per modificare una regola di controllo degli accessi

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Scegliere Access control rules (Regole di controllo accessi).
4. Selezionare la regola da modificare.
5. Scegliere Edit rule (Modifica regola).
6. Modificare la descrizione, l'effetto e le condizioni, secondo necessità.
7. Scegli Save changes (Salva modifiche).

> **Important**
>
> Quando si modifica una regola di accesso, le cassette postali interessate possono impiegare cinque minuti per seguire la regola aggiornata. I client che accedono alle cassette postali

interessate potrebbero mostrare un comportamento incoerente durante quel periodo. Tuttavia, vedrete immediatamente il comportamento corretto quando testate le vostre regole. Per ulteriori informazioni sulle regole di test, consulta i passaggi nella sezione successiva.

Test delle regole di controllo degli accessi

Per vedere come vengono applicate le regole di controllo degli accessi della tua organizzazione, prova le regole dalla WorkMail console Amazon.

Per testare le regole di controllo degli accessi per l'organizzazione

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Scegliere Access control rules (Regole di controllo accessi).
4. Scegliere Test rules (Testa regole).
5. Per Request context (Contesto richiesta), selezionare il protocollo per cui eseguire il test.
6. Per Source IP address (Indirizzo IP di origine), immettere l'indirizzo IP da testare.
7. Per Richiesta eseguita da, scegli il ruolo Utente o Impersonificazione per cui eseguire il test.
8. Seleziona il ruolo utente o di impersonificazione per cui eseguire il test.
9. Scegli Test (Esegui test).

I risultati del test vengono visualizzati sotto Effect (Effetto).

Eliminazione delle regole di controllo degli accessi

Elimina le regole di controllo degli accessi che non ti servono più dalla WorkMail console Amazon.

> **Warning**
>
> Se un amministratore elimina tutte le regole di controllo degli accessi per un'organizzazione, Amazon WorkMail blocca tutti gli accessi alle caselle di posta dell'organizzazione.

Per eliminare una regola di controllo degli accessi

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Scegliere Access control rules (Regole di controllo accessi).
4. Selezionare la regola da eliminare.
5. Scegliere Delete rule (Elimina regola).
6. Scegliere Delete (Elimina).

Impostazione delle policy di conservazione delle mailbox

Puoi impostare politiche di conservazione delle caselle di posta per la tua WorkMail organizzazione Amazon. Le politiche di conservazione eliminano automaticamente i messaggi e-mail dalle caselle di posta degli utenti dopo un periodo di tempo a tua scelta. È possibile scegliere a quali cartelle delle cassette postali applicare i criteri di conservazione. Inoltre, è possibile scegliere se impostare politiche di conservazione diverse per cartelle diverse. Le policy di conservazione delle mailbox si applicano alle cartelle selezionate in tutte le mailbox dell'utente dell'organizzazione. Gli utenti non possono ignorare le politiche di conservazione.

Per impostare una policy di conservazione delle mailbox

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni,

consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Scegliere Retention policy (Policy di conservazione).
4. Per Folder actions (Operazioni cartella), accanto a ogni cartella della mailbox che si desidera includere nella policy, selezionare Delete (Elimina) oppure Permanently delete (Elimina definitivamente).
5. Inserisci il numero di giorni in cui conservare i messaggi di posta elettronica in ogni cartella della cassetta postale prima di eliminarli.
6. Scegli Save (Salva).

Attendi 48 ore per applicare le politiche di conservazione per la tua organizzazione. Se scegli l'azione Elimina cartella, gli utenti possono recuperare i messaggi e-mail eliminati dall'applicazione WorkMail Web Amazon e dai client supportati. Se scegli l'azione Elimina definitivamente la cartella, i messaggi e-mail non possono essere recuperati dopo l'eliminazione.

Il numero di giorni in cui una politica di conservazione conserva un elemento dipende da quando è stato creato, modificato o spostato. Ad esempio, se un criterio di conservazione elimina gli elementi dopo un anno, il criterio conta i giorni di conservazione a partire dalla data di creazione o dall'ultima azione intrapresa su quell'elemento. Non è influenzata dalla data di implementazione della politica di conservazione.

Utilizzo dei domini

Puoi configurare Amazon WorkMail per utilizzare un dominio personalizzato. Puoi anche impostare un dominio come predefinito per la tua organizzazione e abilitarlo AutoDiscover per Microsoft Outlook.

Argomenti

Aggiunta di un dominio

Puoi aggiungere fino a 100 domini alla tua WorkMail organizzazione Amazon. Quando aggiungi un nuovo dominio, una politica di autorizzazione all'invio di Amazon Simple Email Service (Amazon SES) viene aggiunta automaticamente alla politica di identità del dominio. Ciò fornisce WorkMail ad Amazon l'accesso a tutte le azioni di invio di Amazon SES per il tuo dominio e ti consente di reindirizzare le e-mail verso il tuo dominio. Puoi anche reindirizzare le e-mail verso domini esterni.

> **Note**
>
> È consigliabile aggiungere alias per `<postmaster@ e <abuse@>>` a tutti i domini. È possibile creare gruppi di distribuzione per questi alias se si desidera che utenti specifici dell'organizzazione ricevano la posta inviata a tali alias.

Quando configuri la tua WorkMail organizzazione Amazon con un dominio personalizzato, ricorda quanto segue sui record DNS del tuo dominio:

- Per i record CNAME MX e autodiscover, consigliamo di impostare il valore Time to Live (TTL) su 3600. La riduzione del TTL garantisce che i server di posta non utilizzino record MX obsoleti o non validi dopo l'aggiornamento di tali record o la migrazione delle caselle di posta.
- Dopo aver creato gli utenti e i gruppi di distribuzione e aver eseguito correttamente la migrazione delle caselle di posta, è necessario aggiornare il record MX per iniziare a inoltrare le e-mail ad Amazon. WorkMail L'elaborazione degli aggiornamenti ai record DNS può richiedere fino a 48 ore.
- Alcuni provider DNS aggiungono automaticamente i nomi di dominio alle estremità dei record DNS. L'aggiunta di un record che contiene già il nome di dominio, ad esempio _amazonses.example.com, potrebbe comportare la duplicazione del nome di dominio, ottenendo _amazonses.example.com.example.com. Per evitare la duplicazione del nome del dominio nel nome del record, aggiungi un punto alla fine del nome di dominio nel record DNS. Ciò indica al tuo provider DNS che il nome del record è completo e non più relativo al nome di dominio. Impedisce inoltre al provider DNS di aggiungere un ulteriore nome di dominio.
- I nomi di record copiati includono il nome di dominio. A seconda del servizio DNS utilizzato, il nome del dominio potrebbe già essere stato aggiunto al record DNS del dominio.
- Dopo aver creato un record DNS, scegli l'icona di aggiornamento sulla WorkMail console Amazon per visualizzare lo stato di verifica e il valore del record. Per ulteriori informazioni sulla verifica dei domini, consulta Verifica dei domini.
- Ti consigliamo di configurare il tuo dominio come dominio. `MAIL FROM` Per abilitarlo AutoDiscover per i dispositivi iOS, devi configurare il tuo dominio come `MAIL FROM` dominio. Puoi vedere lo stato del tuo `MAIL FROM` dominio nella sezione Migliora la deliverability della console. Per ulteriori informazioni, consulta Configurazione di un dominio MAIL FROM personalizzato.

Per aggiungere un dominio

1. Accedi a AWS Management Console e apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.
2. Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

3. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione a cui desideri aggiungere un dominio.
4. Nel riquadro di navigazione, scegli Domini, quindi scegli Aggiungi dominio.
5. Nella schermata Aggiungi dominio, inserisci un nome di dominio. I nomi di dominio possono contenere solo caratteri latini di base (ASCII).

> **Note**
>
> Se hai un dominio gestito in una zona ospitata pubblica di Amazon Route 53, puoi sceglierlo dal menu a discesa che appare quando inserisci un nome di dominio.

6. Scegli Add domain (Aggiungi dominio).

Viene visualizzata una pagina con l'elenco dei record DNS per il nuovo dominio. La pagina raggruppa i record nelle seguenti sezioni:

- Proprietà del dominio
- WorkMail configurazione
- Sicurezza migliorata
- Invio delle e-mail migliorato

Ciascuna di queste sezioni contiene uno o più record DNS e ogni record mostra un valore di stato. L'elenco seguente mostra i record e i relativi valori di stato disponibili.

Proprietà del file TXT

Verificato: record risolto e verificato.

In sospeso: record non ancora verificato.

Fallito: impossibile verificare la proprietà. Record non corrispondente o non raggiungibile.

WorkMail Configurazione MX

Verificato: record risolto e verificato.

Mancante: impossibile risolvere il record.

Incoerente: il valore non corrisponde al record previsto.

AutoDiscover

Verificato: record risolto e verificato.

Mancante: impossibile risolvere il record.

Incoerente: il valore non corrisponde al record previsto.

> **Note**
>
> Il processo AutoDiscover di verifica verifica anche la corretta AutoDiscover configurazione. Il processo verifica le impostazioni di configurazione per ogni fase. Al termine della verifica viene visualizzato un segno di spunta verde accanto a Verificato nella colonna Stato. Puoi passare il mouse su Verificato e vedere quale delle fasi è stata verificata dal processo. Per ulteriori informazioni sulle AutoDiscover fasi, consultaAbilitazione AutoDiscover alla configurazione degli endpoint.

DIMM CNAME

Verificato: record risolto e verificato.

In sospeso: record non ancora verificato

Fallito: impossibile verificare la proprietà. Record non corrispondente o non raggiungibile.

Per ulteriori informazioni sulla firma DKIM, consulta Authenticating email with DKIM in Amazon SES nella Amazon Simple Email Service Developer Guide.

TESTO SPF

Verificato: record risolto e verificato.

Mancante: impossibile risolvere il record.

Incoerente: il valore non corrisponde al record previsto.

Per ulteriori informazioni sulla verifica SPF, consulta Autenticazione delle e-mail con SPF.

DMARC (TESTO)

Verificato: record risolto e verificato.

Mancante: impossibile risolvere il record.

Incoerente: il valore non corrisponde al record previsto

Per ulteriori informazioni sui record DMARC in Amazon WorkMail, consulta Conformarsi a DMARC con Amazon SES nella Amazon Simple Email Service Developer Guide.

TXT MAIL FROM dal dominio

Verificato: record risolto e verificato.

In sospeso: record non ancora verificato.

Fallito: impossibile verificare la proprietà. Record non corrispondente o non raggiungibile.

Dominio MX MAIL FROM

Verificato: record risolto e verificato.

Mancante: impossibile risolvere il record.

Incoerente: il valore non corrisponde al record previsto.

7. Per il passaggio successivo, scegli l'azione appropriata in base al provider DNS che utilizzi.

   Se utilizzi un dominio Route 53

   - Nella parte superiore della pagina, scegli Aggiorna tutto in Route 53.

   Se utilizzi un altro provider DNS

   - Copia i record e incollali nel tuo provider DNS. Puoi copiare i record in blocco o uno alla volta. Per copiare i record in blocco, scegli Copia tutto. Questo crea una zona di file che puoi importare nel tuo provider DNS. Per copiare i record uno alla volta, scegli i quadrati sovrapposti accanto al nome del record, quindi incollali ciascuno nel tuo provider DNS.

8. Scegli l'icona di aggiornamento per aggiornare lo stato di ogni record. Ciò verifica la proprietà del dominio e la corretta configurazione del tuo dominio con Amazon WorkMail.

Eliminazione di un dominio

È possibile eliminare un dominio quando non se ne ha più bisogno. Tuttavia, devi prima eliminare tutti gli individui o i gruppi che utilizzano il dominio come indirizzo e-mail.

Per eliminare un dominio

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Nome della regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nell'elenco dei domini, spunta la casella di controllo accanto al nome del dominio e seleziona Remove (Elimina).
4. Nella finestra di dialogo Rimuovi dominio, inserisci il nome del dominio da rimuovere e scegli Rimuovi.

Selezione del dominio predefinito

Puoi impostare un dominio associato alla tua organizzazione come predefinito per utenti e gruppi di quell'organizzazione. L'impostazione di un dominio come predefinito non comporta la modifica degli indirizzi e-mail esistenti.

Per impostare un dominio come predefinito

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Nome della regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nell'elenco dei domini, seleziona la casella di controllo accanto al nome di dominio che desideri utilizzare e scegli Imposta come predefinito.

Verifica dei domini

Devi verificare il tuo dominio dopo averlo aggiunto nella WorkMail console Amazon. La verifica del dominio conferma che sei il proprietario del dominio e utilizzerai Amazon WorkMail come servizio di posta elettronica per il dominio.

Verifica un dominio aggiungendo record TXT e MX nel tuo servizio DNS. I record TXT consentono di aggiungere note al servizio DNS. I record MX specificano il server di posta in arrivo.

Usa la console Amazon SES per creare i record TXT e MX, quindi usi la WorkMail console Amazon per aggiungere i record al tuo servizio DNS. Segui questi passaggi.

Per creare record TXT e MX

1. Apri la console Amazon SES all'indirizzo https://console.aws.amazon.com/ses/.
2. Nel riquadro di navigazione, scegli Domini, quindi scegli Verifica un nuovo dominio.

   Viene visualizzata la finestra di dialogo Verifica un nuovo dominio.
3. Nella casella Dominio, inserisci il nome del dominio che hai creato nella Aggiunta di un dominio sezione.
4. (Facoltativo) Se desideri utilizzare DomainKeys Identified Mail (DKIM), seleziona la casella di controllo Genera impostazioni DKIM.
5. Scegli Verify This Domain (Verifica questo dominio).

   La console visualizza un elenco di record TXT e MX.
6. Scegli il link Scarica il set di record come CSV, che si trova sotto l'elenco TXT.

   Viene visualizzata la finestra di dialogo Salva con nome. Scegliete una posizione per il download, quindi scegliete Salva.
7. Apri il file CSV scaricato e copia tutto il suo contenuto.

Una volta creati i record TXT e MX, li aggiungi al tuo provider DNS. I passaggi seguenti utilizzano Route 53. Se utilizzi un provider DNS diverso e non sai come aggiungere record, consulta la documentazione del provider.

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

2. Nel riquadro di navigazione scegliere Hosted Zones (Zone ospitate). Quindi, scegli il pulsante di opzione accanto al dominio che desideri verificare.
3. Dall'elenco dei record DNS per il tuo dominio, scegli Importa file di zona.
4. In File di zona, incolla i record copiati nella casella di testo. Sotto la casella di testo viene visualizzato un elenco dei file.
5. Scorri verso il basso fino alla fine dell'elenco e scegli Importa.

> **Note**
>
> Attendi fino a 72 ore per completare il processo di verifica.

Verifica dei record TXT e MX con il servizio DNS

Conferma che il record TXT che verifica che il dominio sia di tua proprietà venga aggiunto correttamente al servizio DNS. Questa procedura si avvale dello strumento nslookup, disponibile per Windows e Linux. In Linux è possibile usare anche dig.

Per utilizzare lo `nslookup` strumento, devi prima trovare i server DNS che servono il tuo dominio. Quindi, interroghi quei server per visualizzare i record TXT. Puoi interrogare i server DNS per il tuo dominio perché tali server contengono la maggior parte delle up-to-date informazioni relative al tuo dominio. Queste informazioni possono richiedere tempo per la propagazione ad altri server DNS.

Usa nslookup per verificare che il tuo record TXT sia aggiunto al tuo servizio DNS

1. Trova i name server del tuo dominio:
   a. Apri un prompt dei comandi (Windows) o un terminale (Linux).
   b. Esegui il comando seguente per elencare tutti i name server che servono il tuo dominio. *`example.com`*Sostituiscilo con il tuo dominio.

      ```
      nslookup -type=NS example.com
      ```

      Nella fase successiva eseguirai una query su uno di questi name server.
2. Verifica che il record Amazon WorkMail TXT sia stato aggiunto correttamente.

a. Esegui il comando seguente, sostituendolo *example.com* con il tuo dominio e *ns1.name-server.net* con un name server del passaggio 1.

```
nslookup -type=TXT _amazonses.example.com ns1.name-server.net
```

b. Controlla la `"text ="` stringa mostrata nell'output dinslookup. Verifica che questa stringa corrisponda al valore TXT del tuo dominio nell'elenco dei mittenti verificati nella console Amazon WorkMail.

Nell'esempio seguente, vuoi vedere un record TXT per _amazonses.example.com con un valore di. `fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk=` Se aggiorni il record correttamente, il comando ha il seguente risultato:

```
_amazonses.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
```

Usa dig per verificare che il tuo record TXT sia aggiunto al tuo servizio DNS

1. Apri una sessione terminale.
2. Esegui il comando seguente per elencare i record TXT del tuo dominio. *example.com*Sostituiscilo con il tuo dominio.

```
dig +short example.com txt
```

3. Verifica che la stringa che segue TXT nell'output del comando corrisponda al valore TXT visualizzato quando selezioni il dominio nell'elenco dei mittenti verificati della console Amazon WorkMail.

Per usare nslookup per verificare che il record MX venga aggiunto al servizio DNS

1. Trova i server di nomi per il dominio:

a. Apri un prompt dei comandi.

b. Esegui il comando seguente per elencare tutti i name server del tuo dominio.

```
nslookup -type=NS example.com
```

Nel passaggio successivo eseguirai una query su uno di questi name server.

2. Verifica che il record MX sia stato aggiunto correttamente:

   a. Esegui il comando seguente, sostituendolo *example.com* con il tuo dominio e *ns1.name-server.net* con uno dei name server identificati nel passaggio precedente.

   ```
   nslookup -type=MX example.com ns1.name-server.net
   ```

   b. Nell'output del comando, verifica che la stringa che segue `mail exchange =` corrisponda a uno dei seguenti valori:

   Regione Stati Uniti orientali (Virginia settentrionale) — `10 inbound-smtp.us-east-1.amazonaws.com`

   Regione Stati Uniti occidentali (Oregon) — `10 inbound-smtp.us-west-2.amazonaws.com`

   Regione Europa (Irlanda) — `10 inbound-smtp.eu-west-1.amazonaws.com`

   > **Note**
   >
   > `10` rappresenta il numero o priorità della preferenza MX.

Usa dig per verificare che il tuo record MX sia stato aggiunto al tuo servizio DNS

1. Apri una sessione terminale.
2. Esegui il comando seguente per elencare i record MX del tuo dominio.

   ```
   dig +short example.com mx
   ```

3. Verifica che la stringa che segue `MX` corrisponda a uno dei seguenti valori:

   Regione Stati Uniti orientali (Virginia settentrionale) — `10 inbound-smtp.us-east-1.amazonaws.com`

   Regione Stati Uniti occidentali (Oregon) — `10 inbound-smtp.us-west-2.amazonaws.com`

   Regione Europa (Irlanda) — `10 inbound-smtp.eu-west-1.amazonaws.com`

> **Note**
>
> `10` rappresenta il numero o priorità della preferenza MX.

Risoluzione dei problemi di verifica del dominio

Per risolvere i problemi più comuni relativi alla verifica del dominio, consulta i seguenti suggerimenti:

Il tuo servizio DNS non consente caratteri di sottolineatura nei nomi di record TXT

Ometti `_amazonses` dal nome del record TXT.

Vuoi verificare lo stesso dominio più volte ma non puoi avere più record TXT con lo stesso nome

Se il tuo servizio DNS non ti consente di avere più record TXT con lo stesso nome, utilizza una delle seguenti soluzioni alternative:

- (Consigliato) Se il servizio DNS lo consente, assegnate più valori al record TXT. Ad esempio, se il tuo DNS è gestito da Amazon Route 53, puoi impostare più valori per lo stesso record TXT come segue:
  1. Nella console Route 53, scegli il record `_amazonses` TXT che hai aggiunto quando hai verificato il dominio nella prima regione.
  2. Per Value (Valore), premi Enter (Invio) dopo il primo valore.
  3. Aggiungi il valore per la regione aggiuntiva e salva il set di record.
- Se devi verificare il dominio solo due volte, puoi verificarlo una volta creando un record TXT con `_amazonses` il nome e quindi creare un altro record senza `_amazonses` il nome del record.

La WorkMail console Amazon segnala che la verifica del dominio non è riuscita

Amazon non WorkMail riesce a trovare il record TXT necessario per il tuo servizio DNS. Verifica che il record TXT richiesto sia stato aggiunto correttamente al tuo servizio DNS seguendo la procedura riportata in. Verifica dei record TXT e MX con il servizio DNS

Il tuo provider DNS ha aggiunto il nome di dominio alla fine del record TXT

L'aggiunta di un record TXT che contiene già il nome di dominio, ad esempio _amazonses.example.com, può comportare la duplicazione del nome di dominio, ad esempio _amazonses.example.com.example.com. Per evitare la duplicazione del nome del dominio nel nome del record, aggiungi un punto alla fine del nome di dominio nel record TXT. Ciò indica al tuo

provider DNS che il nome del record è completamente qualificato e che il nome di dominio è già incluso nel record TXT.

Amazon WorkMail segnala che il record MX non è coerente

Durante la migrazione da server di posta esistenti, il record MX potrebbe restituire lo stato Incoerente. Aggiorna il tuo record MX in modo che punti ad Amazon WorkMail anziché al server di posta precedente. Il record MX viene inoltre restituito come Inconsistente quando un proxy di posta elettronica di terze parti viene utilizzato insieme ad Amazon WorkMail. In questo caso, è possibile ignorare l'avvertenza Incongruente in sicurezza.

Abilitazione AutoDiscover alla configurazione degli endpoint

AutoDiscover consente di configurare Microsoft Outlook e i client mobili utilizzando solo l'indirizzo e-mail e la password. Il servizio mantiene una connessione ad Amazon WorkMail e aggiorna le impostazioni locali ogni volta che modifichi gli endpoint o le impostazioni. Inoltre, AutoDiscover consente al cliente di utilizzare WorkMail funzionalità Amazon aggiuntive, come la rubrica offline, l' Out-of-OfficeAssistente e la possibilità di visualizzare il tempo libero/occupato in Calendar.

Il client esegue le seguenti AutoDiscover fasi per rilevare l'endpoint del server: URLs

- Fase 1: il client esegue una ricerca SCP (Secure Copy Protocol) nell'Active Directory locale. Se il client non appartiene al dominio, salta questo passaggio. AutoDiscover
- Fase 2: il client invia una richiesta a quanto segue URLs e convalida i risultati. Questi endpoint sono disponibili solo tramite HTTPS.
  - https:///autodiscover/autodiscover.xml *`company.tld`*
  - https://autodiscover. *`company.tld`*/autodiscover/autodiscover.xml
- Fase 3 — Il client esegue una ricerca DNS su autodiscover.company.tld e invia una richiesta GET non autenticata all'endpoint derivato dall'indirizzo e-mail dell'utente. Se il server restituisce un reindirizzamento 302, il client invia nuovamente la richiesta sull'endpoint HTTPS restituito. AutoDiscover

Se tutte queste fasi falliscono, il client non può essere configurato automaticamente. Per ulteriori informazioni sulla configurazione manuale di dispositivi mobili consulta l'argomento relativo alla connessione manuale del dispositivo.

Ti viene richiesto di aggiungere il record AutoDiscover DNS al tuo provider quando aggiungi il dominio ad Amazon. WorkMail Ciò consente al client di eseguire la fase 3 del AutoDiscover processo. Tuttavia, questi passaggi non funzionano per tutti i dispositivi mobili, come l'app di posta elettronica Android di serie. Di conseguenza, potrebbe essere necessario configurare la AutoDiscover fase 2 manualmente.

Puoi utilizzare i seguenti metodi per configurare la AutoDiscover fase 2 per il tuo dominio:

(Consigliato) Usa Route 53 e Amazon CloudFront

> **Note**
>
> I passaggi seguenti spiegano come creare un proxy per https://autodiscover. *`company.tld`*/autodiscover/autodiscover.xml. Per creare un proxy per https://*`company.tld`*/autodiscover/autodiscover.xml, rimuovi il prefisso dai domini nei `autodiscover.` passaggi seguenti. L'utilizzo CloudFront di Route 53 può comportare costi. Per ulteriori informazioni sui prezzi applicabili, consulta i prezzi di Amazon e CloudFront i prezzi di Amazon Route 53.

Per abilitare la AutoDiscover fase 2 con Route 53 e CloudFront

1. Ottieni un certificato SSL per l'autodiscovery. *`company.tld`*e caricalo su AWS Identity and Access Management (IAM) o. AWS Certificate Manager Per ulteriori informazioni, consulta Lavorare con i certificati del server nella Guida per l'utente IAM o Guida introduttiva nella Guida per l'AWS Certificate Manager utente.
2. Crea una nuova CloudFront distribuzione:
    1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
    2. Nel riquadro di navigazione seleziona Distributions (Distribuzioni).
    3. Scegliere Create Distribution (Crea distribuzione).
    4. In Web, scegli Inizia.
    5. In Impostazioni Origin, inserisci i seguenti valori:
        - Nome di dominio di origine: il nome di dominio appropriato per la tua regione:
            - Stati Uniti orientali (Virginia settentrionale) — **`autodiscover-service.mail.us-east-1.awsapps.com`**
            - Stati Uniti occidentali (Oregon) — **`autodiscover-service.mail.us-west-2.awsapps.com`**

- Europa (Irlanda) — **`autodiscover-service.mail.eu-west-1.awsapps.com`**

- Politica del protocollo di origine: la politica desiderata: **`Match Viewer`**

> **Note**
>
> Lascia vuoto il percorso di Origin. Non modificare il valore compilato automaticamente per Origin ID.

6. Nelle impostazioni predefinite del comportamento della cache, seleziona i seguenti valori per le impostazioni elencate:
   - Viewer Protocol Policy (Criteri protocollo visualizzatore): HTTPS Only (Solo HTTPS)
   - Allowed HTTP Methods (Metodi HTTP consentiti): GET, HEAD, OPTIONS, POST, PUT, PATCH, DELETE
   - Cache Based on Selected Request Headers (Cache in base a intestazioni richiesta selezionate): All (Tutte)
   - Forward Cookie (Inoltra cookie): All (Tutti)
   - Query String Forwarding and Caching (Inoltro e caching di stringhe di query): None (Improves Caching) (Nessuno (migliora caching))
   - Smooth Streaming: No
   - Restrict Viewer Access (Limita accesso visualizzatore): No
7. Selezionare i seguenti valori per Distribution Settings (Impostazioni distribuzione):
   - Price Class (Categoria prezzo): Use only US, Canada, and Europe (Usa soltanto Stati Uniti, Canada ed Europa)
   - Per Nomi di dominio alternativi (CNAMEs), inserisci **`autodiscover.`*`company.tld`*** o***`company.tld`***, *`company.tld`* dov'è il tuo nome di dominio.
   - Certificato SSL: certificato SSL personalizzato (archiviato in IAM)
   - Custom SSL Client Support (Supporto client SSL personalizzato): scegliere All Clients (Tutti i client) o Only Clients that Support Server Name Indication (SNI) (Solo client che supportano Server Name Indication (SNI)). Le versioni precedenti di Android potrebbero non funzionare con quest'ultima opzione.

> **Note**
>
> Se si sceglie All Clients (Tutti i client), lasciare Default Root Object (Oggetto root di default) vuoto.

- Logging (Registrazione): scegliere On (Attivata) o Off (Disattivata). Attivato abilita la registrazione.
- Per Comment (Commento), inserire **`AutoDiscover type2 for autodiscover.`*`company.tld`***
- Stato di distribuzione: scegli Abilitato.

8. Scegliere Create Distribution (Crea distribuzione).

3. Nella console Route 53, crea un record che indirizza il traffico Internet dal tuo nome di dominio alla tua CloudFront distribuzione.

> **Note**
>
> Questi passaggi presuppongono che il record DNS per example.com sia ospitato su Route 53. Se non utilizzi Route 53, segui le procedure nella console di gestione del tuo provider DNS.

1. Nel pannello di navigazione della console, scegli Hosted Zones, quindi scegli un dominio.
2. Nell'elenco dei domini, scegli il nome di dominio che desideri utilizzare.
3. In Record, scegli Crea record.
4. In Record di creazione rapida, imposta i seguenti parametri:
   - In Nome record, inserisci un nome per il record.
   - In Politica di routing, seleziona Routing semplice.
   - Scegli il cursore Alias per attivarlo. Il cursore diventa blu quando è acceso.
   - Nell'elenco Tipo di record, scegli A - Indirizza il traffico verso un IPv4 indirizzo e alcune risorse AWS.
   - Nell'elenco Instrada il traffico verso la distribuzione, scegli Alias alla CloudFront distribuzione.

- Apparirà una casella di ricerca sotto l'elenco Route traffic to. Inserisci il nome della tua CloudFront distribuzione nella casella di testo. Puoi anche selezionare la tua distribuzione dall'elenco che appare quando selezioni la casella di ricerca.

5. Scegli Crea record.

Usa un server web Apache

I passaggi seguenti spiegano come utilizzare un server Web Apache per creare un proxy per https://autodiscover.*company.tld*/autodiscover/autodiscover.xml. Per creare un proxy per https:///autodiscover/autodiscover.xml, rimuovi «autodiscover». *company.tld* dai domini seguendo le fasi sotto riportate.

Per abilitare la AutoDiscover fase 2 con un server web Apache

1. Esegui le seguenti direttive su un server Apache abilitato per SSL:

```
SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
```

2. Se necessario, abilita i seguenti moduli Apache. Se non sai come fare, consulta l'aiuto di Apache:

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`
   - `ssl`

Consulta la sezione seguente per informazioni su test e risoluzione dei problemi AutoDiscover.

AutoDiscover fase 2: risoluzione dei problemi

Dopo aver configurato il provider DNS per AutoDiscover, puoi testare la AutoDiscover configurazione degli endpoint. Se hai configurato correttamente l'endpoint, questo risponde con un messaggio di richiesta non autorizzato.

Per effettuare una richiesta non autorizzata di base

1. Da un terminale, crea una richiesta POST non autenticata sull'endpoint. AutoDiscover

```
$ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
autodiscover.xml
```

Se l'endpoint è configurato correttamente, dovrebbe restituire un `401 unauthorized` messaggio, come mostrato nell'esempio seguente:

```
$ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
autodiscover.xml
...
HTTP/1.1 401 Unauthorized
```

2. Successivamente, verifica una AutoDiscover richiesta reale. Create un `request.xml` file con il seguente contenuto XML:

```
<?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. Usa il `request.xml` file che hai creato ed effettua una AutoDiscover richiesta autenticata all'endpoint. Ricordati di sostituire *`testuser@company.tld`* con un indirizzo email valido:

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

La risposta sarà simile al seguente esempio se l'endpoint è configurato correttamente:

```
$ 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>
```

Modifica delle policy d'identità del dominio

Le politiche di identità del dominio specificano le autorizzazioni per le azioni e-mail, come il reindirizzamento dei messaggi e-mail. Ad esempio, puoi reindirizzare le e-mail a qualsiasi indirizzo e-mail della tua WorkMail organizzazione Amazon.

> **Note**
>
> A partire dal 1° aprile 2022, Amazon WorkMail ha iniziato a utilizzare i principali di servizio per l'autorizzazione anziché i principali dell' AWS account. Se hai aggiunto un dominio prima del 1° aprile 2022, potresti avere una politica precedente che utilizza un AWS account principal per l'autorizzazione. In tal caso, ti consigliamo di eseguire l'aggiornamento alla politica più recente. I passaggi di questa sezione spiegano come. L'organizzazione continua a inviare e-mail normalmente durante l'aggiornamento.

Segui questi passaggi solo se non utilizzi una policy Amazon SES personalizzata. Se utilizzi una policy Amazon SES personalizzata, devi aggiornarla tu stesso. Per ulteriori informazioniPolicy principale del servizio Amazon SES personalizzata, consulta la sezione più avanti in questo argomento.

> **Important**
>
> Non rimuovere i domini esistenti. Se lo fai, interromperai il servizio di posta. Tutto quello che devi fare è reinserire i domini esistenti.

Per aggiornare una politica di identità del dominio

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. A tale scopo, apri l'elenco Seleziona una regione, situato a destra della casella di ricerca, quindi scegli la regione desiderata. Per ulteriori informazioni sulle regioni, consulta Regioni ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizzazioni, quindi scegli il nome dell'organizzazione.
3. Nel riquadro di navigazione, scegli Domini.
4. Evidenzia e copia il nome del dominio che desideri reinserire, quindi scegli Aggiungi dominio.

   Viene visualizzata la finestra di dialogo Aggiungi dominio.
5. Incolla il nome copiato nella casella Nome dominio, quindi scegli Aggiungi dominio.
6. Ripeti i passaggi 3-5 per i domini rimanenti dell'organizzazione.

Policy principale del servizio Amazon SES personalizzata

Se utilizzi una policy Amazon SES personalizzata, adatta questo esempio per utilizzarlo nel tuo dominio.

```
{
  "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"
        }
      }
    }
  ]
}
```

Autenticazione delle e-mail con SPF

Il Sender Policy Framework (SPF) è uno standard di convalida di e-mail, progettato per combattere lo spoofing delle e-mail. Lo spoofing è l'atto di far sembrare un'e-mail inviata da un malintenzionato un'e-mail inviata da un utente legittimo. Per informazioni sulla configurazione di SPF per il tuo dominio WorkMail abilitato ad Amazon, consulta Authenticating email with SPF in Amazon SES.

Configurazione di un dominio MAIL FROM personalizzato

Per impostazione predefinita, Amazon WorkMail utilizza un sottodominio di amazonses.com come `MAIL FROM` dominio per le e-mail in uscita. Ciò può causare errori di consegna se la politica DMARC sul tuo dominio è impostata solo per SPF. Per risolvere questo problema, configura il tuo dominio come dominio. `MAIL FROM` Per informazioni su come configurare il tuo dominio e-mail come `MAIL FROM` dominio, consulta Configurazione di un dominio MAIL FROM personalizzato nella Amazon Simple Email Service Developer Guide.

> **Important**
>
> È necessario un dominio MAIL FROM personalizzato quando si abilita AutoDiscover per i dispositivi iOS.

Per ulteriori informazioni sui `MAIL FROM` domini personalizzati, consulta Amazon SES ora supporta i domini MAIL FROM personalizzati.

Operazioni con gli utenti

Puoi creare e rimuovere utenti da Amazon WorkMail. Inoltre, puoi reimpostare le loro password e-mail, gestire le quote delle caselle di posta e l'accesso ai dispositivi e controllare le autorizzazioni delle loro caselle di posta.

Argomenti

Visualizzazione di un elenco di utenti

Per visualizzare l'elenco degli utenti

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel pannello di navigazione, seleziona Utenti.
4. Inoltre, puoi filtrare gli utenti per nome utente, nome visualizzato o indirizzo email principale.

> **Note**
>
> La ricerca distingue tra maiuscole e minuscole.

Aggiunta di un utente

Quando aggiungi un utente, Amazon crea WorkMail automaticamente delle caselle di posta per lui. Gli utenti possono effettuare il login e accedere alla propria posta dall'applicazione WorkMail web Amazon, dal proprio dispositivo mobile o utilizzando Microsoft Outlook su macOS o PC.

Aggiunta di un utente

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli l'organizzazione a cui desideri aggiungere utenti.
3. Nel riquadro di navigazione, scegli Utenti, quindi scegli Aggiungi utente.

   Viene visualizzata la schermata Aggiungi un utente.
4. In Dettagli utente, nel campo Nome utente, inserisci il nome dell'utente. Il nome viene visualizzato anche nella casella Indirizzo e-mail. Se desideri che l'utente abbia un indirizzo e-mail diverso dal nome utente, puoi modificare il campo Indirizzo e-mail.
5. (Facoltativo) Inserisci il nome e il cognome dell'utente nelle caselle Nome e Cognome.
6. Nella casella Nome visualizzato, inserisci il nome visualizzato dell'utente.
7. Nella casella Indirizzo e-mail, accetta l'alias e-mail o inseriscine un altro.
8. Per impostazione predefinita, gli utenti vengono visualizzati nell'elenco globale degli indirizzi. Per nascondere l'utente dall'elenco di indirizzi globale, deselezionare la casella di controllo Mostra nell'elenco indirizzi globale.
9. Seleziona Non creare una cassetta postale per aggiungere un utente come utente remoto all'organizzazione.

10. In Configurazione della password, inserisci la password dell'utente nelle caselle Password e Ripeti password.
11. Scegli Add user (Aggiungi utente).

Abilitare gli utenti

Quando integri Amazon WorkMail con la tua Active Directory aziendale o hai già utenti disponibili nella tua directory Simple AD, puoi abilitare tali utenti in Amazon WorkMail. Segui questi passaggi anche per riabilitare un utente il cui account è stato disabilitato.

Per abilitare gli utenti

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizzazioni, quindi scegli l'organizzazione per la quale desideri abilitare gli utenti.
3. Nel pannello di navigazione, seleziona Utenti.

   Viene visualizzato un elenco di utenti. Gli account utente negli stati abilitato, disabilitato e utente di sistema sono visualizzati nell'elenco.
4. Dall'elenco degli utenti con account disabilitati, seleziona le caselle di controllo relative agli utenti che desideri abilitare, quindi scegli Abilita.

   Viene visualizzata la finestra di dialogo Abilita utenti.
5. Se necessario, rivedi e modifica l'indirizzo e-mail principale per ogni utente, quindi scegli Abilita.

Gestione degli alias utente

Puoi aggiungere o rimuovere alias e-mail per gli utenti.

Per aggiungere un alias e-mail a un utente

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione per cui desideri aggiungere utenti.
3. Nel riquadro di navigazione, scegli Utenti, quindi seleziona il nome dell'utente a cui desideri aggiungere un alias.
4. Nella sezione Dettagli utente, scegli la scheda Alias.
5. Nella scheda Alias, scegli Aggiungi alias.
6. Nella casella Alias, inserisci un alias.
7. Seleziona un dominio per un alias.
8. Scegli Aggiungi.

Per rimuovere un alias e-mail da un utente

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione da cui desideri rimuovere gli utenti.
3. Nel riquadro di navigazione, scegli Utenti, quindi seleziona il nome dell'utente da cui desideri rimuovere gli alias.
4. Nella sezione Dettagli utente, scegli la scheda Alias.
5. Nella scheda Alias, seleziona la casella di controllo corrispondente agli alias che desideri rimuovere.
6. Verifica gli alias che verranno rimossi.
7. Nella finestra Rimuovi alias, scegli Rimuovi.

Disabilitazione di utenti

Puoi disabilitare qualsiasi utente di un'organizzazione in qualsiasi momento. Quando si disabilita un utente, questo diventa immediatamente inaccessibile. Gli utenti disattivati per più di 30 giorni vedranno la loro casella di posta eliminata da Amazon WorkMail.

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli l'organizzazione che contiene gli utenti che desideri disabilitare.
3. Nel pannello di navigazione, seleziona Utenti.

   Viene visualizzato un elenco di tutti gli utenti, che mostra gli account che si trovano negli stati abilitato, disabilitato e utente di sistema.
4. Dall'elenco degli utenti abilitati, seleziona le caselle di controllo relative agli account che desideri disabilitare, quindi scegli Disabilita.

   Viene visualizzata la finestra di dialogo Disabilita utenti.
5. Scegliere Disabilita.

Modifica dei dettagli dell'utente

Quando modifichi i dettagli dell'utente, puoi modificare quanto segue:

- Dati personali: nomi, indirizzo e-mail, numeri di telefono e altri dettagli personali.
- Quote (dimensioni) delle caselle di posta: le quote possono variare da 1 MB a 51.200 MB (50 GB). Amazon WorkMail avvisa gli utenti quando raggiungono il 90% della loro quota. Inoltre, la modifica della quota di caselle di posta di un utente non influirà sui prezzi. Per ulteriori informazioni sui prezzi, consulta la pagina WorkMail dei prezzi di Amazon.
- Accesso ai dispositivi mobili: rimuovi e cancella i dati dei dispositivi e visualizza i dettagli del dispositivo.

- Autorizzazioni di accesso alla cassetta postale: concedi agli utenti l'autorizzazione a utilizzare una casella di posta e concedi agli utenti diversi livelli di accesso alla cassetta postale.
- Token di accesso personali (quando IAM Identity Center è abilitato): visualizza ed elimina i token di accesso personali.

> **Note**
>
> Se integri Amazon WorkMail con una directory AD Connector, non puoi modificare questi dettagli da AWS Management Console. Invece, devi modificarli utilizzando gli strumenti di gestione di Active Directory. Le limitazioni si applicano quando l'organizzazione è in modalità di interoperabilità. Per ulteriori informazioni, consulta Limitazioni nella modalità di interoperabilità.

Per modificare i dettagli dell'utente

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizzazioni, quindi scegli l'organizzazione che desideri utilizzare.
3. Nel riquadro di navigazione, scegli Utenti, quindi scegli il nome dell'utente da modificare.

Per modificare i dati personali

1. Nella sezione Dettagli utente, scegli Modifica.
2. In Dettagli utente, inserisci o modifica le informazioni personali dell'utente secondo necessità.
3. Al termine, scegli Salva modifiche.

Da associare a un utente IAM Identity Center

1. In Dettagli utente, scegli Modifica.

2. Inserisci l'ID utente dell'utente IAM Identity Center che desideri associare. Puoi visualizzare queste informazioni nella tabella Utenti assegnati nella pagina IAM Identity Center o nella console IAM Identity Center.
3. Scegli Save changes (Salva modifiche).

Per modificare le quote delle cassette postali

1. In Dettagli utente, scegli la scheda Quota, quindi scegli Modifica.
2. Nella casella Aggiorna quota della casella di posta, inserisci una dimensione per la casella di posta. È possibile inserire valori da a**1**. **51200**
3. Scegli Save changes (Salva modifiche).

Per gestire i dati dei dispositivi mobili

> **Note**
>
> Per gestire i dispositivi mobili, i tuoi utenti devono prima connettere i loro dispositivi alla tua istanza di Amazon WorkMail. Per informazioni sulla connessione dei dispositivi mobili, consulta Configurazione dei client per dispositivi mobili per Amazon WorkMail.

1. In Dettagli utente, scegli la scheda Dispositivi mobili.
2. Per visualizzare l'elenco corrente dei dispositivi, scegli Aggiorna.
3. Per visualizzare i dettagli di un dispositivo, scegli il nome del dispositivo dalla colonna ID dispositivo.
4. Per rimuovere o cancellare il dispositivo, scegli il pulsante di opzione accanto al nome del dispositivo, quindi scegli Rimuovi o Cancella se necessario.
5. Nella finestra di dialogo visualizzata, confermate l'operazione di rimozione o cancellazione. Ricorda che gli utenti riappariranno quando sincronizzeranno WorkMail nuovamente i loro dispositivi con Amazon.

Per modificare le autorizzazioni della casella di posta

1. Scegli la scheda Autorizzazioni.
2. Completa una delle seguenti operazioni:

1. Per aggiungere autorizzazioni, scegli Aggiungi autorizzazioni. Apri l'elenco Aggiungi nuove autorizzazioni e scegli un utente o un gruppo, scegli le impostazioni di autorizzazione per l'utente o il gruppo, quindi scegli Salva.
2. Per modificare le autorizzazioni utente, scegli il pulsante accanto al nome dell'utente. Scegliete Modifica, selezionate le opzioni desiderate, quindi scegliete Salva.

Per ulteriori informazioni sulle opzioni di autorizzazione, consultaUtilizzo delle autorizzazioni della casella di posta.

3. Per rimuovere tutte le autorizzazioni, scegli Rimuovi, quindi conferma la rimozione.

Per eliminare i token di accesso personali

> **Note**
>
> Assicurati che il token che stai eliminando non venga utilizzato attivamente da nessun client di posta elettronica. L'eliminazione di un token quando è in uso interromperà l'autenticazione per i client che utilizzano il token.

1. Scegli la scheda Token di accesso personali.
2. Dall'elenco dei token di accesso personali, seleziona il token di accesso personale da eliminare.
3. Scegli Elimina token.
4. Inserisci Tipo nella casella di testo di conferma.

Reimpostazione della password dell'utente

Se un utente dimentica la password o ha problemi di accesso ad Amazon WorkMail, puoi reimpostarla.

> **Note**
>
> - Se hai integrato Amazon WorkMail con una directory AD Connector, devi reimpostare la password utente in Active Directory.

- Se hai integrato Amazon WorkMail con IAM Identity Center, puoi scegliere di reimpostare la password utente. Per ulteriori informazioni, consulta Reimpostazione della password utente di IAM Identity Center per un utente finale nella Guida per l'AWS IAM Identity Center utente.

Per reimpostare la password di un utente

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel pannello di navigazione, seleziona Utenti.
4. Nell'elenco degli utenti, seleziona la casella di controllo accanto al nome dell'utente, quindi scegli Reimposta password.
5. Nella finestra di dialogo Reimposta password, inserisci la nuova password, quindi scegli Reimposta.

Risoluzione dei problemi relativi alle politiche WorkMail sulle password di Amazon

Se la reimpostazione della password non riesce, verificare che la nuova password soddisfi i requisiti della policy sulle password.

I requisiti della politica in materia di password dipendono dal tipo di directory utilizzato dalla tua WorkMail organizzazione Amazon.

Politica sulle password di Amazon WorkMail Directory e Simple AD

Per impostazione predefinita, le password per una WorkMail directory Amazon o una directory Simple AD devono essere:

- Non vuota

- Almeno otto caratteri
- Meno di 64 caratteri
- Composto da caratteri supplementari in latino di base o Latin-1

Le password devono contenere caratteri da tre su cinque dei gruppi seguenti:

- Caratteri maiuscoli
- Caratteri minuscoli
- Cifre numeriche (da 0 a 9)
- Caratteri speciali (ad esempio, <, ~ o !)
- Caratteri Latin-1 Supplement (ad esempio, é, ü o ñ)

Le politiche relative WorkMail alle password di Amazon Directory non possono essere modificate.

Per modificare una politica di password Simple AD, utilizza gli strumenti di amministrazione AD su un'istanza Windows Amazon Elastic Compute Cloud (Amazon EC2) della tua directory Simple AD. Per ulteriori informazioni, consulta Installazione degli strumenti di amministrazione di Active Directory nella Guida all'AWS Directory Service amministrazione.

AWS Managed Microsoft AD Politica relativa alle password delle directory

Per informazioni sulla politica di password predefinita per una AWS Managed Microsoft AD directory, vedere Manage Password Policies AWS Managed Microsoft AD nella AWS Directory Service Administration Guide.

Criteri relativi alle password di AD Connector

AD Connector utilizza la politica delle password del dominio Active Directory a cui è connesso. Consulta la documentazione del tuo dominio Active Directory per ulteriori informazioni sulle impostazioni delle politiche relative alle password.

Utilizzo delle notifiche

Con l'API Amazon WorkMail Push Notifications, puoi ricevere notifiche push sulle modifiche nella tua casella di posta, inclusi nuovi aggiornamenti di e-mail e calendario. Devi registrare il URLs (o i risponditori di notifiche push) per ricevere le notifiche. Con questa funzionalità, gli sviluppatori

possono creare applicazioni reattive per WorkMail gli utenti Amazon, in quanto le applicazioni ricevono rapidamente notifiche sulle modifiche dalla casella di posta dell'utente.

Per ulteriori informazioni consultare l'articolo relativo alle notifiche per sottoscrizioni, eventi di mailbox e EWS in Exchange.

Puoi iscriverti a cartelle specifiche, come Posta in arrivo o Calendario, o a tutte le cartelle per gli eventi di modifica della cassetta postale (inclusi New Mail, Created e Modified).

È possibile utilizzare librerie client come EWS Java API o Managed EWS C# API per accedere a questa funzionalità. Un'applicazione di esempio completa di un risponditore push, sviluppata utilizzando AWS Lambda e API Gateway (utilizzando il framework AWS Serverless), è disponibile sulla pagina. AWS GitHub Utilizza l'API per Java di EWS.

Di seguito è riportato un esempio di richiesta di sottoscrizione push:

```
<?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>
```

Di seguito è riportato un risultato di richiesta di sottoscrizione andata a buon fine:

```
<?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>
```

Successivamente le notifiche vengono inviate agli URL specificati nella richiesta di sottoscrizione. Di seguito è riportata una notifica di esempio:

```
<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>
```

Per riconoscere che il risponditore delle notifiche push ha ricevuto la notifica, deve rispondere nel modo seguente:

```
<?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>
```

Per annullare la ricezione delle notifiche push, i client devono inviare una risposta di annullamento della sottoscrizione nel campo `SubscriptionStatus` in maniera analoga a come riportato di seguito:

```
<?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>
```

Per verificare lo stato del tuo risponditore di notifiche push, Amazon WorkMail invia un «battito cardiaco» (chiamato anche a`StatusEvent`). La frequenza con cui vengono inviati dipende dal parametro `StatusFrequency` fornito nella richiesta di sottoscrizione iniziale. Ad esempio, se è `StatusFrequency` uguale**1**, a `StatusEvent` viene inviato ogni minuto. Questo valore può essere compreso tra 1 e 1440 minuti. Questo `StatusEvent` ha il seguente aspetto:

```
<?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>
```

Se un client che risponde alle notifiche push non risponde con `OK` lo stesso stato di prima, la notifica viene ritentata per un massimo di minuti. `StatusFrequency` Ad esempio, se `StatusFrequency` è uguale a 5 e la prima notifica ha esito negativo, viene effettuato un altro tentativo per un massimo di 5 minuti con un backoff esponenziale tra ogni tentativo. Se la notifica non viene recapitata dopo

la scadenza del periodo di riprova, l'abbonamento viene invalidato e non vengono inviate nuove notifiche. È necessario creare una nuova sottoscrizione per continuare a ricevere le notifiche relative agli eventi della mailbox. Al momento è possibile effettuare la sottoscrizione per un massimo di tre sottoscrizioni per mailbox.

Abilitazione di e-mail crittografate o firmate

È possibile utilizzare S/MIME per consentire agli utenti di inviare e-mail firmate o crittografate sia all'interno che all'esterno dell'organizzazione.

> **Note**
>
> I certificati utente nell'Elenco indirizzi globale (GAL) sono supportati solo in una configurazione Active Directory connessa.

Per abilitare gli utenti a inviare e-mail crittografate o firmate

1. Configura un Active Directory (AD) Connector. La configurazione di un AD Connector con la tua directory locale consente agli utenti di continuare a utilizzare le loro credenziali aziendali esistenti.
2. Configura la registrazione automatica dei certificati per emettere e archiviare automaticamente i certificati utente in Active Directory. Amazon WorkMail riceve i certificati utente da Active Directory e li pubblica nel GAL. Per ulteriori informazioni, consulta Configurazione della registrazione automatica dei certificati.
3. Distribuisci i certificati generati agli utenti esportando i certificati dal server che esegue Microsoft Exchange e inviandoli per posta.
4. Ogni utente installa il certificato per il proprio programma e-mail (ad esempio Windows Outlook) e dispositivi mobili.

Utilizzo di gruppi

Puoi utilizzare i gruppi come liste di distribuzione in Amazon WorkMail per ricevere e-mail per indirizzi e-mail generici, come `<sales@example.com>` o `<support@example.com>`. È possibile creare più alias di e-mail per un gruppo.

Puoi anche utilizzare i gruppi come gruppi di sicurezza per condividere un calendario o una casella di posta con un determinato team.

I gruppi non dispongono di cassette postali proprie e ciò influisce sulle autorizzazioni delle cassette postali che puoi concedere a un gruppo. Per informazioni sulla configurazione delle autorizzazioni delle cassette postali per un gruppo, vedere. Gestione delle autorizzazioni delle cassette postali per i gruppi

> **Note**
>
> Possono essere necessarie fino a 2 ore prima che i gruppi appena aggiunti appaiano nella rubrica offline di Microsoft Outlook.

Argomenti

Visualizzazione di un elenco di gruppi

Per visualizzare l'elenco dei gruppi

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, selezionare Groups (Gruppi).
4. Inoltre, puoi filtrare i gruppi in base al nome del gruppo o all'indirizzo email principale.

> **Note**
>
> La ricerca distingue tra maiuscole e minuscole.

Aggiungere un gruppo

Puoi aggiungere gruppi dalla WorkMail console Amazon.

Per aggiungere un gruppo

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modifica la regione AWS Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Gruppi, quindi scegli Aggiungi gruppo.

   Viene visualizzata la pagina Aggiungi gruppo.
4. In Nome gruppo, inserisci un nome per il gruppo.
5. In Indirizzo e-mail, inserisci l'indirizzo e-mail principale del gruppo.
6. Verifica l'indirizzo e-mail del gruppo, aggiornalo se necessario.

7. Per impostazione predefinita, il gruppo viene visualizzato nell'elenco di indirizzi globale. Per nascondere il gruppo dall'elenco di indirizzi globale, deselezionare la casella di controllo Mostra nell'elenco indirizzi globale.
8. Scegliere Add Group (Aggiungi gruppo).

Abilitare i gruppi

Quando integri Amazon WorkMail con il tuo Active Directory aziendale o hai già gruppi disponibili nel tuo Active Directory semplice, puoi utilizzare tali gruppi come gruppi di sicurezza o liste di distribuzione in Amazon WorkMail.

Per abilitare un gruppo di directory esistente

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, selezionare Groups (Gruppi).
4. Seleziona la casella di controllo accanto al gruppo che desideri abilitare, quindi scegli Abilita.

   Viene visualizzata la finestra di dialogo Abilita gruppi che chiede di confermare l'operazione.
5. Se necessario, rivedi e modifica l'indirizzo e-mail principale per ogni gruppo, quindi scegli Abilita.

Aggiungere membri a un gruppo

Dopo aver creato e abilitato un WorkMail gruppo Amazon, usa la WorkMail console Amazon per aggiungere membri a quel gruppo.

> **Note**
>
> Se Amazon WorkMail è integrato con un servizio Active Directory connesso o Microsoft Active Directory, puoi utilizzare Active Directory per gestire i membri del tuo gruppo. Tuttavia, la propagazione delle modifiche su Amazon WorkMail può richiedere più tempo.

Per aggiungere membri a un gruppo

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, selezionare Groups (Gruppi).
4. Selezionare il nome del gruppo.
5. Nella pagina dei dettagli del gruppo, scegli la scheda Membri.
6. Scegli un gruppo o un utente da aggiungere in Gruppo o Utente.
7. Seleziona l'utente o il gruppo dal menu a discesa.
8. Seleziona Salva.

La propagazione delle modifiche può richiedere alcuni minuti.

Modifica dei dettagli del gruppo

Puoi modificare i dettagli di un gruppo.

Per modificare i dettagli del gruppo

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Gruppi, quindi seleziona il gruppo da modificare.
4. Nella pagina dei dettagli del gruppo, aggiorna l'indirizzo e-mail in base alle esigenze.

5. Per impostazione predefinita, i gruppi vengono visualizzati nell'elenco di indirizzi globale. Per nascondere il gruppo dall'elenco di indirizzi globale, deselezionare la casella di controllo Mostra nell'elenco indirizzi globale.
6. Scegli Save changes (Salva modifiche).

Rimuovere membri da un gruppo

Usa la WorkMail console Amazon per rimuovere membri da un gruppo.

> **Note**
>
> Se Amazon WorkMail è integrato con un'Active Directory o Microsoft Active Directory connessa, puoi utilizzare Active Directory per gestire i membri del tuo gruppo. Tuttavia, così facendo puoi creare il tempo necessario per propagare le modifiche su Amazon WorkMail.

Per rimuovere membri da un gruppo

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Gruppi, quindi scegli il nome del gruppo.
4. Nella pagina dei dettagli del gruppo, scegli la scheda Membri.
5. Seleziona il membro da rimuovere dal gruppo.
6. Scegli Rimuovi.

La propagazione delle modifiche può richiedere alcuni minuti.

Gestione degli alias di gruppo

Puoi aggiungere o rimuovere alias e-mail ai gruppi.

Per aggiungere un alias e-mail a un gruppo.

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione per cui desideri aggiungere un alias.
3. Nel riquadro di navigazione, scegli Gruppi, quindi seleziona il nome del gruppo a cui desideri aggiungere un alias.
4. Nella sezione Dettagli del gruppo, scegli Alias.
5. In Alias, scegli Aggiungi alias.
6. Nella casella Alias, inserisci un alias.
7. Seleziona un dominio per un alias.
8. Scegli Aggiungi.

Per rimuovere un alias di posta elettronica da un gruppo.

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione da cui desideri rimuovere un alias.
3. Nel riquadro di navigazione, scegli Gruppi, quindi seleziona seleziona il nome del gruppo da cui desideri rimuovere gli alias.
4. Nella sezione Dettagli del gruppo, scegli Alias.
5. In Alias, seleziona la casella di controllo corrispondente agli alias che desideri rimuovere.
6. Scegli Rimuovi.
7. Verifica gli alias che verranno rimossi.

8. Nella finestra Rimuovi alias, scegli Rimuovi.

Disabilitazione dei gruppi

Puoi eliminare un gruppo quando non ne hai più bisogno.

Per disabilitare un gruppo

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, selezionare Groups (Gruppi).
4. In Nome gruppo, seleziona i gruppi da disabilitare, quindi scegli Disabilita.
5. Nella finestra di dialogo Disable group(s) (Disabilita gruppo(i)), seleziona Disable (Disabilita).

Eliminazione di un gruppo

Prima di poter eliminare un gruppo, devi prima disabilitare quel gruppo. Per informazioni sulla disabilitazione dei gruppi, vedereDisabilitazione dei gruppi.

Per eliminare un gruppo

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, selezionare Groups (Gruppi).
4. Seleziona la casella di controllo accanto al gruppo di disabili che desideri eliminare e scegli Elimina.

Viene visualizzata la finestra di dialogo Elimina.

5. Nella casella Inserisci il nome del gruppo per confermare l'eliminazione, inserisci il nome del gruppo, quindi scegli Elimina.

> **Note**
>
> Per eliminare definitivamente un gruppo, utilizza l'azione `DeleteGroup` API per Amazon WorkMail. Per ulteriori informazioni, DeleteGroupconsulta Amazon WorkMail API Reference.

Utilizzo delle risorse

Amazon WorkMail può aiutare i tuoi utenti a prenotare risorse. Ad esempio, gli utenti possono prenotare sale riunioni o apparecchiature come proiettori, telefoni o automobili. Per prenotare una risorsa, l'utente aggiunge la risorsa all'invito alla riunione.

Argomenti

Visualizzazione di un elenco di risorse

Per visualizzare l'elenco delle risorse

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di spostamento seleziona Resources (Risorse).
4. Inoltre, puoi filtrare le risorse in base al nome della risorsa o all'indirizzo email principale.

> **Note**
>
> La ricerca distingue tra maiuscole e minuscole.

Aggiungere una risorsa

Puoi aggiungere una nuova risorsa alla tua organizzazione e consentire agli utenti di prenotarla.

Per aggiungere una risorsa

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Risorse, quindi Aggiungi risorsa.

   Viene visualizzata la pagina Aggiungi risorsa.
4. Nella casella Nome risorsa, inserisci un nome per la risorsa.
5. Facoltativamente, nella casella Descrizione risorsa, immettere una descrizione per la risorsa.
6. In Tipo di risorsa, scegli un'opzione.
7. Verifica l'indirizzo email della risorsa, aggiorna se necessario.
8. Per impostazione predefinita, la risorsa viene visualizzata nell'elenco indirizzi globale. Per nascondere la risorsa dall'elenco di indirizzi globale, deselezionare la casella di controllo Mostra nell'elenco indirizzi globale.
9. Scegliere Add resource (Aggiungi risorsa).

Modifica dei dettagli delle risorse

Puoi modificare i dettagli generali di una risorsa, tra cui nome, descrizione, tipo e indirizzo e-mail, opzioni di prenotazione e delegati.

Per modificare i dettagli delle risorse generali

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni,

consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di spostamento selezionare Resources (Risorse), quindi selezionare la risorsa da modificare.
4. Nella pagina dei dettagli della risorsa, aggiorna il nome della risorsa, la descrizione, il tipo di risorsa o l'indirizzo e-mail in base alle esigenze.
5. Per impostazione predefinita, le risorse vengono visualizzate nell'elenco globale degli indirizzi. Per nascondere la risorsa dall'elenco di indirizzi globale, deselezionare la casella di controllo Mostra nell'elenco indirizzi globale.
6. Scegli Save changes (Salva modifiche).

È possibile configurare una risorsa in modo da accettare o rifiutare automaticamente le richieste di prenotazione.

Puoi modificare le opzioni di prenotazione della risorsa.

Per modificare le opzioni di prenotazione di una risorsa

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di spostamento selezionare Resources (Risorse), quindi selezionare la risorsa da modificare. Viene visualizzata una pagina con i dettagli della risorsa.
4. In Opzioni di prenotazione scegli Modifica.
5. Se necessario, seleziona o deseleziona la casella di controllo accanto a un'opzione per abilitare o disabilitare l'opzione.

> **Note**
>
> Quando disabiliti una qualsiasi delle opzioni di prenotazione automatica, devi creare un delegato per gestire le richieste di prenotazione. I passaggi successivi spiegano come creare un delegato.

Puoi aggiungere un delegato per controllare le richieste di prenotazione per una risorsa per cui non sono configurate opzioni di prenotazione automatiche. I delegati delle risorse ricevono automaticamente le copie di tutte le richieste di prenotazione e hanno accesso completo al calendario delle risorse. Inoltre, devono accettare tutte le richieste di prenotazione per una risorsa.

Per aggiungere un delegato per una risorsa

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Risorse, quindi seleziona il nome della risorsa a cui desideri aggiungere un delegato.
4. (Facoltativo) Nella scheda Opzioni di prenotazione, scegli Modifica, deseleziona la casella di controllo Accetta automaticamente tutte le richieste di risorse e quindi scegli Salva.
5. Scegli la scheda Delegati, quindi scegli Aggiungi delegato.

   Viene visualizzata la finestra di dialogo Aggiungi delegato.
6. Apri l'elenco dei delegati di ricerca e scegli un delegato, quindi scegli Salva.

Per rimuovere un delegato alle risorse

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni,

consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione da cui desideri rimuovere i delegati.
3. Nel riquadro di navigazione, scegli Risorse, quindi seleziona il nome della risorsa da cui desideri rimuovere un delegato.
4. Scegli Delegati, quindi scegli il delegato da rimuovere.
5. Scegli Rimuovi.

Gestione degli alias delle risorse

Puoi aggiungere o rimuovere alias e-mail alle risorse.

Per aggiungere un alias e-mail a una risorsa

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione a cui desideri aggiungere un alias.
3. Nel riquadro di navigazione, scegli Risorse, quindi seleziona il nome della risorsa a cui desideri aggiungere un alias.
4. Nella sezione Dettagli delle risorse, scegli Alias.
5. In Alias, scegli Aggiungi alias.
6. Nella casella Alias, inserisci un alias.
7. Seleziona un dominio per un alias.
8. Scegli Aggiungi.

Per rimuovere un alias di posta elettronica da una risorsa

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione da cui desideri rimuovere gli alias.
3. Nel riquadro di navigazione, scegli Risorse, quindi seleziona il nome della risorsa da cui desideri rimuovere gli alias.
4. Nella sezione Dettagli delle risorse, scegli Alias.
5. In Alias, seleziona la casella di controllo corrispondente agli alias che desideri rimuovere.
6. Scegli Rimuovi.
7. Verifica gli alias che verranno rimossi.
8. Nella finestra Rimuovi alias, scegli Rimuovi.

Abilitare una risorsa

Per impostazione predefinita, Amazon WorkMail crea una risorsa. Se tu o qualcun altro disabilitate una risorsa, potete riattivarla entro 30 giorni.

Per abilitare una risorsa

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni sulle regioni, consulta Regioni ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli l'organizzazione che contiene la risorsa che desideri abilitare.
3. Nel riquadro di spostamento seleziona Resources (Risorse).
4. Nell'elenco delle risorse, seleziona il pulsante accanto alla risorsa che desideri abilitare, quindi scegli Abilita.

   Viene visualizzata la finestra di dialogo Abilita risorsa.
5. Scegli Abilita .

Disabilitazione di una risorsa

Quando disabiliti una risorsa, la rendi non disponibile per la prenotazione. Ad esempio, puoi disabilitare una sala conferenze mentre è in fase di ristrutturazione, quindi abilitare la sala quando è disponibile per l'uso.

Per disabilitare una risorsa

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni sulle regioni, consulta Regioni ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli l'organizzazione che contiene la risorsa che desideri disabilitare.
3. Nel riquadro di spostamento seleziona Resources (Risorse).
4. Nell'elenco delle risorse, seleziona il pulsante accanto alla risorsa che desideri disabilitare, quindi scegli Disabilita.

   Viene visualizzata la finestra di dialogo Disabilita risorsa.
5. Scegliere Disabilita.

Eliminazione di una risorsa

Quando una risorsa non ti serve più, puoi eliminarla. Tuttavia, devi prima disabilitare la risorsa. Per informazioni sulla disabilitazione di una risorsa, consulta la procedura descritta nella sezione precedente.

Per rimuovere una risorsa

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni sulle regioni, consulta Regioni ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizzazioni, quindi scegli l'organizzazione desiderata.
3. Nel riquadro di spostamento seleziona Resources (Risorse).

4. Nell'elenco delle risorse, seleziona il pulsante accanto alla risorsa disattivata che desideri rimuovere, quindi scegli Elimina.

   Viene visualizzata la finestra di dialogo Elimina risorsa.

5. Nella casella Immetti il nome della risorsa per confermare l'eliminazione, immetti il nome della risorsa che desideri eliminare, quindi scegli Elimina risorsa.

Lavorare con IAM Identity Center

Puoi abilitare l'autenticazione a più fattori (MFA) in Amazon associando i tuoi utenti WorkMail WorkMail Amazon a IAM Identity Center. Per ulteriori informazioni, consulta Cos'è IAM Identity Center.

La tabella seguente descrive i passaggi per affrontare diversi scenari.

Scenario	Fasi
Associazione WorkMail degli utenti Amazon a IAM Identity Center	1. Abilitazione di IAM Identity Center in Amazon WorkMail 2. Assegnazione di utenti e gruppi IAM Identity Center all'applicazione Amazon WorkMail 3. Associazione WorkMail degli utenti Amazon agli utenti di IAM Identity Center
WorkMail Utenti Amazon esistenti	1. Crea utenti IAM Identity Center con lo stesso nome utente, raggruppa gli utenti e assegna il gruppo all' WorkMail applicazione Amazon. 2. Associa gli WorkMail utenti Amazon agli utenti di IAM Identity Center.
Utenti IAM Identity Center esistenti	1. Crea WorkMail utenti Amazon con lo stesso nome utente degli utenti di IAM Identity Center. 2. Assegna gli utenti o i gruppi di IAM Identity Center all' WorkMailapplicazione Amazon. 3. Associa gli WorkMail utenti Amazon agli utenti di IAM Identity Center.
Connessione di una directory esterna a IAM Identity Center	1. Sincronizza gli utenti della directory esterna con il gruppo IAM Identity Center. Per ulteriori informazioni, consulta i tutorial sui sorgenti di IAM Identity Center Identity

Scenario	Fasi
	2. Assegna il gruppo IAM Identity Center all' WorkMail applicazione Amazon. 3. Connetti la directory esterna ad Amazon WorkMail e assicurati che i nomi utente corrispondano 4. Associa gli WorkMail utenti Amazon agli utenti di IAM Identity Center.

Una volta completati i passaggi precedenti, puoi visualizzare lo stato dell'IAM Identity Center, collegarti a AWS IAM Identity Center per gestire utenti e gruppi, l'URL dell'applicazione WorkMail web Amazon abilitata per MFA, la modalità di autenticazione, lo stato del token di accesso personale e la cronologia in IAM Identity Center in Impostazioni nella console Amazon. WorkMail Per ulteriori informazioni sulla gestione della MFA nella console IAM Identity Center, consulta Autenticazione a più fattori per gli utenti di IAM Identity Center.

> **Note**
>
> Assicurati che la configurazione tra Amazon WorkMail e IAM Identity Center sia ben testata e verificata. Gli utenti potrebbero perdere l'accesso alle proprie caselle di posta quando la configurazione non è corretta e completa.

Argomenti

- Abilitazione di IAM Identity Center in Amazon WorkMail
- Assegnazione di utenti e gruppi IAM Identity Center all'applicazione Amazon WorkMail
- Associazione WorkMail degli utenti Amazon agli utenti di IAM Identity Center
- Modalità di autenticazione
- Configurazione dei token di accesso personali
- Disabilitazione di IAM Identity Center

Abilitazione di IAM Identity Center in Amazon WorkMail

Quando abiliti IAM Identity Center, funge da livello di autenticazione per gli WorkMail utenti Amazon. Gli utenti di IAM Identity Center vengono gestiti separatamente dalla WorkMail directory Amazon. Si consiglia di utilizzare gli stessi nomi utente su IAM Identity Center e Amazon WorkMail.

> **Note**
>
> Assicurati che Amazon WorkMail e IAM Identity Center siano configurati nella stessa regione.

Per abilitare IAM Identity Center, segui questi passaggi.

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Identity Center.

   Viene visualizzata la pagina delle impostazioni di IAM Identity Center.
3. Scegli Abilita .

   Viene visualizzata la finestra Abilita IAM Identity Center.
4. Scegli Abilita .

   Viene visualizzata la pagina delle impostazioni dell'Identity Center con lo stato dell'Identity Center.
5. Per aggiungere utenti e gruppi IAM Identity Center alla tua WorkMail organizzazione Amazon, segui il link sotto Identity Center status. Per informazioni su come aggiungere utenti e gruppi, consulta Gestire le identità in IAM Identity Center. .

Assegnazione di utenti e gruppi IAM Identity Center all'applicazione Amazon WorkMail

Quando abiliti IAM Identity Center in Amazon WorkMail, WorkMail crea un'applicazione in IAM Identity Center per tuo conto. Per impostazione predefinita, gli utenti di IAM Identity Center devono

essere assegnati a questa applicazione o appartenere a un gruppo assegnato a questa applicazione per accedere a una casella di posta nell' WorkMailorganizzazione Amazon. Per ulteriori informazioni, consulta le applicazioni AWS gestite nella Guida per l' AWS IAM Identity Center utente.

Puoi assegnare utenti e gruppi di IAM Identity Center ad Amazon WorkMail nei seguenti modi:

- Dagli utenti di IAM Identity Center: puoi assegnare gli utenti di IAM Identity Center ad Amazon WorkMail.
- Per gruppo IAM Identity Center: puoi assegnare gruppi IAM Identity Center ad Amazon WorkMail. Aggiungendo un gruppo, tutti gli utenti di un gruppo avranno accesso ad Amazon WorkMail.

  Per ulteriori informazioni sull'aggiunta di utenti e gruppi, consulta Utenti, gruppi e provisioning in IAM Identity Center.

> **Note**
>
> Se stai collegando la tua fonte di identità esistente con IAM Identity Center, consulta quanto segue prima di modificare l'origine della directory.
>
> - L'autenticazione viene gestita da IAM Identity Center.
> - Amazon WorkMail manterrà tutti gli WorkMail utenti e i gruppi Amazon.
> - IAM Identity Center manterrà tutti gli utenti, i gruppi e le assegnazioni di IAM Identity Center.
> - Devi gestire WorkMail gli utenti e i gruppi Amazon nella WorkMail console Amazon.
> - È necessario gestire gli utenti e i gruppi di IAM Identity Center in IAM Identity Center.
> - Gli utenti senza un'assegnazione o un'associazione di utenti IAM Identity Center non possono accedere ad Amazon WorkMail.
> - È necessario gestire i controlli delle policy MFA in IAM Identity Center.
> - Quando modifichi l'origine di IAM Identity Center da e verso Manage Active Directory in IAM Identity Center, devi disabilitare le configurazioni IAM Identity Center esistenti in Amazon WorkMail e riconfigurarle per associare i tuoi WorkMail utenti Amazon a IAM Identity Center.

Gli utenti e i gruppi sincronizzati con la tua directory IAM Identity Center possono essere assegnati alla tua applicazione Amazon WorkMail. Per ulteriori informazioni sulla gestione di utenti e gruppi di IAM Identity Center, consulta Introduzione alle attività comuni in IAM Identity Center. .

Per assegnare utenti e gruppi di IAM Identity Center ad Amazon WorkMail, segui questi passaggi.

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Identity Center.

   Viene visualizzata la pagina delle impostazioni di IAM Identity Center.
3. Seleziona Assegna utenti e gruppi.

   Puoi aggiungere e assegnare nuovi utenti o assegnare utenti e gruppi esistenti.

   - Assegna utenti: puoi assegnare singoli utenti di IAM Identity Center ad Amazon. WorkMail Puoi creare un nuovo utente IAM Identity Center o cercare un utente esistente.
   - Assegna gruppi: puoi anche assegnare un gruppo IAM Identity Center ad Amazon. WorkMail Tutti i membri del gruppo verranno quindi assegnati ad Amazon WorkMail.

> **Note**
>
> Tutti i nuovi utenti di IAM Identity Center sono abilitati per impostazione predefinita in IAM Identity Center. Per concedere l'accesso ad Amazon WorkMail, devi impostare la loro password in IAM Identity Center e assegnarla ad Amazon WorkMail. Per ulteriori informazioni, consulta Aggiungere utenti alla directory di Identity Center.

Associazione WorkMail degli utenti Amazon agli utenti di IAM Identity Center

Quando un utente accede al client WorkMail web Amazon con le proprie credenziali utente IAM Identity Center, il client aprirà la casella di posta dell'utente Amazon WorkMail associato. Se nessun utente dell' WorkMailorganizzazione è associato all'utente IAM Identity Center, WorkMail creerà

un'associazione tra l'utente di IAM Identity Center che effettua l'accesso e l' WorkMail utente con lo stesso nome utente, se tale WorkMail utente esiste. In caso contrario, il client mostrerà un messaggio di errore all'utente.

> **Note**
>
> Ti consigliamo di utilizzare lo stesso nome utente per un utente su Amazon WorkMail e IAM Identity Center perché WorkMail creerà l'associazione automaticamente quando l'utente accede per la prima volta al client WorkMail web Amazon con le proprie credenziali utente IAM Identity Center. Quando i nomi utente sono diversi, sei responsabile della creazione dell'associazione.

Per associare gli utenti, segui questi passaggi.

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Identity Center.

   Viene visualizzata la pagina delle impostazioni di IAM Identity Center.
3. Scegli Associa utenti.
4. In Seleziona un WorkMail utente, seleziona l' WorkMail utente Amazon che desideri associare.
5. In Inserisci l'ID utente IAM Identity Center, inserisci l'ID dell'utente IAM Identity Center che desideri associare. Puoi copiare l'ID dalla scheda Utenti assegnati nella pagina Identity Center.

   > **Note**
   >
   > L'utente IAM Identity Center deve essere autorizzato ad accedere all' WorkMail applicazione Amazon.
6. Scegli Utenti associati.

   Una volta completata l'associazione, l' WorkMail utente Amazon può accedere ad Amazon WorkMail utilizzando le credenziali MFA IAM Identity Center.

> **Note**
>
> Puoi anche associare WorkMail gli utenti Amazon agli utenti IAM Identity Center quando modifichi i dettagli WorkMail utente Amazon. Per ulteriori informazioni, consulta Modifica dei dettagli dell'utente.

Modalità di autenticazione

Puoi utilizzare la modalità di autenticazione per consentire agli utenti di accedere utilizzando le credenziali della WorkMail directory Amazon, le credenziali IAM Identity Center o limitando l'accesso alle sole credenziali IAM Identity Center.

In Amazon sono disponibili due modalità di autenticazione WorkMail.

> **Note**
>
> La scelta della modalità di autenticazione dipende dai requisiti di sicurezza e dalle preferenze di esperienza utente dell'organizzazione. Si consiglia di utilizzare solo la modalità IAM Identity Center in quanto fornisce una maggiore sicurezza applicando le credenziali IAM Identity Center e l'MFA. Tuttavia, prima di passare dalla modalità Amazon WorkMail Directory e IAM Identity Center, assicurati di testare il processo MFA con tutti i tuoi utenti per garantire una transizione fluida ed evitare qualsiasi impatto sull'accesso ai client di posta elettronica esistenti.

- Amazon WorkMail Directory e IAM Identity Center (consigliati per i test): questa è l'opzione predefinita per testare le associazioni di IAM Identity Center prima di passare alla modalità di produzione. La modalità test consente agli utenti di accedere al client WorkMail Web Amazon utilizzando sia la WorkMail directory Amazon che le credenziali IAM Identity Center. Quando condividi l'URL dell'applicazione WorkMail web Amazon dalle impostazioni dell'organizzazione, l'utente può accedere utilizzando le credenziali della WorkMail directory Amazon. Quando condividi l'URL abilitato per MFA dalle impostazioni di IAM Identity Center, l'utente può accedere utilizzando le proprie credenziali IAM.
- Solo IAM Identity Center (consigliato per la produzione): questa modalità di autenticazione consente di accedere alla casella di posta del WorkMail client Amazon solo utilizzando le credenziali IAM Identity Center. Per tutti WorkMail gli utenti Amazon esistenti, le credenziali della

WorkMail directory Amazon non sono più valide sia per l'applicazione WorkMail Web Amazon che per i client di posta elettronica esistenti. Puoi richiedere un token di accesso personale per accedere alla casella di posta utilizzando qualsiasi client di posta elettronica. Per evitare di perdere l'accesso alle caselle di posta, assicurati che l'MFA sia abilitata per tutti gli utenti Amazon WorkMail .

Per abilitare la modalità di autenticazione, segui questi passaggi.

1. Nella pagina Impostazioni Identity Center, scegli la scheda Modalità di autenticazione.
2. Scegli Modifica.

   Viene visualizzata la pagina Modifica modalità di autenticazione.
3. Selezionare uno dei seguenti:

   - Solo IAM Identity Center
   - Amazon WorkMail Directory e IAM Identity Center
4. Scegli Save (Salva).

Configurazione dei token di accesso personali

Puoi abilitare il token di accesso personale per consentire WorkMail agli utenti Amazon di accedere alle loro caselle di posta utilizzando client di posta elettronica desktop e mobili. Dopo aver abilitato IAM Identity Center, per impostazione predefinita, lo stato del token di accesso personale è impostato su attivo ed è valido per 365 giorni. Dopo aver abilitato IAM Identity Center, le credenziali esistenti degli utenti non saranno più valide per accedere ai loro client di posta elettronica. I tuoi utenti possono generare il token di accesso personale dall'applicazione WorkMail web Amazon e utilizzarlo per accedere a qualsiasi client di posta elettronica. Puoi modificare la scadenza del token di accesso personale e quando il token scade, l'utente può generarne uno nuovo.

> **Note**
>
> - Il tuo utente può visualizzare e copiare il tuo token di accesso personale solo una volta quando lo crei in Amazon WorkMail. Se perdi il tuo token di accesso personale, dovrai generarne uno nuovo per motivi di sicurezza.

- Amazon consente i token di accesso personali per l'accesso alle caselle di posta WorkMail solo quando WorkMail l'utente Amazon è associato a un utente IAM Identity Center autorizzato ad accedere all'applicazione Amazon WorkMail.

Le configurazioni dei token di accesso personali sono elencate di seguito:

- Attivo: quando lo stato del token di accesso personale è impostato su Attivo, l'utente può generare un token di accesso personale da Amazon WorkMail e utilizzarlo per accedere a qualsiasi client di posta elettronica entro il periodo di vita del token.
- Inattivo: quando lo stato del token di accesso personale è impostato su Inattivo, l'utente non sarà in grado di generare o utilizzare token di accesso personali per accedere alle caselle di posta.
- Durata del token: per impostazione predefinita, il token di accesso personale è valido per 365 giorni. Hai la possibilità di modificare la durata del token di accesso personale. Se lasci vuota l'impostazione relativa alla durata, il token avrà una durata indefinita e non scadrà mai.

Per configurare i token di accesso personali, segui questi passaggi.

1. Nella pagina Impostazioni Identity Center, scegli la scheda Configurazione del token di accesso personale.
2. Scegli Modifica.

   Viene visualizzata la pagina Modifica configurazione del token personale.
3. In Stato del token, fai scorrere il pulsante Attivo per abilitare il token di accesso personale.
4. Nella casella di testo Durata del token (in giorni), inserisci il numero di giorni in cui il token di accesso personale può essere attivato.
5. Scegli Save (Salva).

Disabilitazione di IAM Identity Center

Puoi disabilitare IAM Identity Center dalla WorkMail console Amazon. Una volta disabilitato, non è possibile accedere alla casella di posta utilizzando le credenziali IAM Identity Center o i token di accesso personali. Si consiglia di reimpostare tutte le password degli utenti e gli WorkMail utenti Amazon torneranno a utilizzare le credenziali di Amazon WorkMail Directory.

> **Note**
>
> Verifica quanto segue:
>
> - Dopo aver disabilitato IAM Identity Center, gli utenti e i gruppi di Amazon WorkMail e IAM Identity Center rimarranno invariati.
> - Le associazioni di utenti esistenti continueranno a esistere.
> - L'autenticazione tornerà a essere gestita da Amazon WorkMail Directory, anziché da IAM Identity Center.

Per disabilitare IAM Identity Center, segui questi passaggi.

1. Nella pagina Impostazioni Identity Center, scegli Disabilita.

   Viene visualizzata la pagina Disabilita IAM Identity Center.
2. Scegli Conferma.

Lavorare con i dispositivi mobili

Gli argomenti di questa sezione spiegano come gestire i dispositivi mobili connessi ad Amazon WorkMail.

Argomenti

Modifica della policy per i dispositivi mobili dell'organizzazione

Puoi modificare le policy relative ai dispositivi mobili della tua organizzazione per cambiare il modo in cui i dispositivi mobili interagiscono con Amazon WorkMail.

Per modificare la policy per i dispositivi mobili dell'organizzazione

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modifica Regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Nome della regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, selezionare Mobile Policies (Policy per i dispositivi mobili), quindi nella schermata Mobile policy (Policy per i dispositivi mobili), selezionare Edit (Modifica).
4. Aggiornare uno dei seguenti se necessario:

   a. Require encryption on device (Richiedi crittografia su dispositivo): esegue la crittografia dei dati di posta sul dispositivo mobile.
   b. Require encryption on storage card (Richiedi crittografia sulla scheda di memoria): esegue la crittografia dei dati di posta nell'archivio rimovibile del dispositivo mobile.
   c. Password richiesta: richiedi una password per sbloccare un dispositivo mobile.
   d. Consenti una password semplice: utilizza il PIN del dispositivo come password.

e. Lunghezza minima della password: imposta il numero di caratteri richiesti per una password valida.

f. Richiedi una password alfanumerica: richiedi password composte da lettere e numeri.

g. Numero di tentativi falliti consentiti: specifica il numero di tentativi falliti di sblocco del dispositivo consentiti prima che il dispositivo dell'utente venga cancellato. Tutti i dati, inclusi i file personali, verranno eliminati quando il dispositivo viene cancellato.

h. Password expiration (Scadenza password): specifica il numero di giorni prima che una password scade e deve essere modificata.

i. Enable screen lock (Abilita blocco schermo): specifica il numero di secondi che deve trascorrere senza l'intervento dell'utente per il blocco dello schermo dell'utente.

j. Enforce password history (Applica cronologia password): specifica il numero di password che possono essere inserite prima di ripetere la stessa password.

5. Seleziona Salva.

Gestione dei dispositivi mobili

Gli argomenti di questa sezione spiegano come cancellare in remoto i dispositivi mobili, rimuovere i dispositivi dall'organizzazione e visualizzare i dettagli dei dispositivi. Per ulteriori informazioni sulla modifica della policy sui dispositivi mobili della tua organizzazione, consulta Modifica della policy per i dispositivi mobili dell'organizzazione.

Argomenti

Cancellazione da remoto dei dispositivi mobili

I passaggi di questa sezione spiegano come cancellare i dati da remoto dai dispositivi mobili. Ricorda quanto segue:

- I dispositivi devono essere online e connessi ad Amazon WorkMail. Se qualcuno disconnette il dispositivo, l'operazione di cancellazione riprende quando l'utente ricollega il dispositivo.
- La propagazione delle operazioni di cancellazione può richiedere cinque minuti.

> **Important**
>
> Per la maggior parte dei dispositivi mobili, una cancellazione remota reimposta le impostazioni di fabbrica. Tutti i dati, inclusi i file personali, possono essere rimossi quando esegui questa procedura.

Per cancellare da remoto il dispositivo mobile di un utente

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modifica Regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta Nome della regione ed endpoint in. Riferimenti generali di Amazon Web Services
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Utenti e nell'elenco degli utenti seleziona il nome dell'utente di cui devi cancellare il dispositivo.
4. Scegli la scheda Dispositivi mobili.
5. Nell'elenco dei dispositivi, scegli il pulsante accanto al dispositivo, quindi scegli Cancella.
6. Controlla lo stato nella panoramica per vedere se è richiesta la cancellazione.
7. Dopo aver cancellato il dispositivo, rimuovilo dall'elenco dei dispositivi. I passaggi riportati nella sezione successiva spiegano come.

   > **Important**
   >
   > Per riportare un dispositivo cancellato nell'elenco dei dispositivi di un utente, assicurati innanzitutto di rimuoverlo dall'elenco dei dispositivi. In caso contrario, il sistema cancella nuovamente il dispositivo.

Rimozione dei dispositivi degli utenti dall'elenco dei dispositivi

Se qualcuno smette di usare uno specifico dispositivo mobile o hai cancellato i dati dal dispositivo da remoto, puoi rimuovere il dispositivo dall'elenco dei dispositivi. Quando l'utente configura di nuovo il dispositivo, verrà visualizzato nell'elenco.

Per rimuovere i dispositivi mobili di un utente dall'elenco di dispositivi

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modifica Regione AWS. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Utenti, quindi seleziona il nome dell'utente.
4. Scegli la scheda Dispositivi mobili.
5. Nell'elenco dei dispositivi, seleziona il pulsante accanto al dispositivo e scegli Rimuovi.

Visualizzazione dei dettagli dei dispositivi mobile

Puoi visualizzare i dettagli del dispositivo mobile di un utente.

> **Note**
>
> Alcuni dispositivi non inviano tutti i dati al server. Potresti non visualizzare tutti i dettagli disponibili sul dispositivo.

Per visualizzare i dettagli del dispositivo

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione . Nella barra di navigazione selezionare la regione che soddisfa le proprie esigenze. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, scegli Utenti, quindi scegli la scheda Dispositivi mobili.
4. Nell'elenco dei dispositivi, seleziona l'ID del dispositivo di cui desideri visualizzare i dettagli.

   La tabella seguente elenca i codici di stato del dispositivo.

Stato	Descrizione
PROVISIONING_REQUIRED	Un utente o un amministratore ha richiesto che il dispositivo venga fornito per l'uso con Amazon WorkMail. I dispositivi vengono impostati su questo stato anche se la politica corrente per quel dispositivo viene modificata nella WorkMail console Amazon.
PROVISIONING_SUCCEEDED	Il provisioning del dispositivo è stato eseguito correttamente. Il dispositivo ha applicato la politica specificata.
WIPE_REQUIRED	Un amministratore ha richiesto una cancellazione nella WorkMail console Amazon.
WIPE_SUCCEEDED	La cancellazione del dispositivo è riuscita.

Gestione delle regole di accesso ai dispositivi mobili

Le regole di accesso ai dispositivi mobili per Amazon WorkMail consentono agli amministratori di controllare l'accesso alle caselle di posta per determinati tipi di dispositivi mobili. Per impostazione predefinita, ogni WorkMail organizzazione Amazon utilizza una regola che concede l'accesso alla casella di posta elettronica a qualsiasi dispositivo, indipendentemente dal tipo, modello, sistema operativo o agente utente. Puoi modificare o sostituire quella regola predefinita con una tua. Puoi anche aggiungere, modificare ed eliminare regole.

> **Warning**
>
> Se elimini tutte le regole di accesso ai dispositivi mobili per un'organizzazione, Amazon WorkMail blocca tutti gli accessi ai dispositivi mobili.

Puoi creare regole che consentono o negano l'accesso in base alle seguenti proprietà del dispositivo:

- Tipo di dispositivo: «iPhone», «iPad» o «Android».

- Modello di dispositivo: «iPhone 10c1", «iPad 5c1" o" X». HTCOne
- Sistema operativo del dispositivo: «iOS 12.3.1 16F203" o «Android 8.1.0».
- Agente utente del dispositivo: «iOS/14.2 (18B92) exchangesyncd/1.0» o «Android-Mail/7.7.16.163886392.release».

Per visualizzare le proprietà del dispositivo sulla console di AWS gestione, vedere Visualizzazione dei dettagli del dispositivo mobile.

> **Note**
>
> Alcuni dispositivi e client potrebbero non riportare le proprietà per tutti i campi. Per informazioni su come aggirare questi casi, vedere Dealing with empty fields

> **Important**
>
> Le regole di accesso ai dispositivi WorkMail mobili di Amazon si applicano solo ai dispositivi che utilizzano il ActiveSync protocollo Microsoft Exchange. I client mobili che utilizzano un protocollo diverso, come IMAP, non segnalano le proprietà del dispositivo elencate qui, quindi queste regole non si applicano.
> Se devi limitare l'accesso ai dispositivi che utilizzano altri protocolli, puoi creare regole di controllo degli accessi. Per ulteriori informazioni su di esse, consulta Lavorare con le regole di controllo degli accessi. Ad esempio, è possibile limitare l'accesso ad altri protocolli e webmail solo a un intervallo di indirizzi IP aziendali, ma consentire l'accesso a Microsoft ActiveSync da altre sedi e quindi utilizzare le regole di accesso ai dispositivi mobili per limitare ulteriormente i tipi e le versioni di client consentiti.

Argomenti

Come funzionano le regole di accesso ai dispositivi mobili

Le regole di accesso ai dispositivi mobili si applicano solo ai dispositivi che utilizzano il ActiveSync protocollo Microsoft Exchange. Ogni regola presenta una serie di condizioni che specificano quando

viene applicata, oltre a un effetto di accesso di `ALLOW` o `DENY` per il dispositivo. Una regola si applica a una richiesta di accesso solo se tutte le condizioni della regola corrispondono alle proprietà del dispositivo mobile dell'utente. Le regole senza condizioni si applicano a tutte le richieste. Ogni condizione utilizza una corrispondenza del prefisso senza distinzione tra maiuscole e minuscole e le proprietà segnalate dal dispositivo.

Amazon WorkMail valuta le regole come segue:

- Se una `DENY` regola corrisponde a una proprietà del dispositivo, la policy blocca il dispositivo. `DENY`le regole hanno la precedenza sulle `ALLOW` regole.
- Se almeno una `ALLOW` regola corrisponde e nessuna `DENY` regola corrisponde, la policy lo consente il dispositivo.
- Se non si applica alcuna regola, il dispositivo viene bloccato.

> **Important**
>
> I dispositivi mobili segnalano le proprietà utilizzate dalle regole per il funzionamento. I dispositivi segnalano le proprie proprietà durante il processo di provisioning dei ActiveSync dispositivi Microsoft. Amazon WorkMail non può verificare in modo indipendente che i client mobili riportino up-to-date informazioni corrette.

Utilizzo delle regole di accesso ai dispositivi mobili

Puoi utilizzare APIs o l'interfaccia a riga di comando (CLI) di AWS per creare e gestire le regole di accesso ai dispositivi mobili. Per ulteriori informazioni su AWS CLI, consulta la AWS Command Line Interface User Guide.

> **Important**
>
> Quando modifichi una regola di accesso per un' WorkMail organizzazione Amazon, i dispositivi interessati possono impiegare cinque minuti per seguire la regola aggiornata e i dispositivi potrebbero mostrare un comportamento incoerente durante quel periodo. Tuttavia, si nota immediatamente il comportamento corretto quando si testano le regole. Per ulteriori informazioni, consulta Testing mobile device access rules.

Elenco delle regole di accesso ai dispositivi mobili

L'esempio seguente mostra come elencare le regole di accesso ai dispositivi mobili.

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Creazione di regole di accesso ai dispositivi mobili

L'esempio seguente crea una regola che impedisce a tutti i dispositivi Android di accedere alle cassette postali.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

L'esempio seguente crea una regola che consente solo una versione specifica di iOS. Assicurati di rimuovere la `ALLOW-all` regola predefinita.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

Aggiornamento delle regole di accesso ai dispositivi mobili

L'esempio seguente aggiorna una regola del dispositivo aggiungendo un identificatore.

```
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"
```

Eliminazione di una regola di accesso ai dispositivi mobili

L'esempio seguente elimina la regola di accesso ai dispositivi mobili con l'identificatore specificato.

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

Test delle regole di accesso ai dispositivi mobili

Per testare le regole di accesso, puoi utilizzare l'GetMobileDeviceAccessEffectAPI o il comando get-mobile-device-access -effect in. AWS CLI Per ulteriori informazioni su AWS CLI, consulta la Guida per l'utente dell'interfaccia a riga di AWS comando.

Quando esegui il test, trasmetti le proprietà di un dispositivo mobile simulato e l'API o la CLI restituiscono l'effetto `ALLOW` di accesso, `DENY` o, che riceverebbe un dispositivo mobile reale con tali proprietà. Ad esempio, questo comando verifica se un iPhone con iOS 14.2, oltre all'app di posta predefinita, può accedere a una cassetta postale.

```
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"
```

Gestione dei campi vuoti

Alcuni dispositivi mobili o client potrebbero non riportare le informazioni per uno o più campi, lasciando i valori vuoti. Le regole possono corrispondere a quelle di questi dispositivi utilizzando il valore speciale `$NONE` in una condizione. Ad esempio, una regola con `DeviceTypes=["iphone", "ipad", "$NONE"]` corrisponderà ai dispositivi che segnalano un tipo di `"iphone"` dispositivo o non segnalano affatto un tipo di dispositivo. `"ipad"`

Condizioni negative come `NotDeviceTypes` o non `NotDeviceUserAgents` corrisponderanno a questi valori vuoti. Ad esempio, una regola con `NotDeviceTypes=["android"]` corrisponderà ai dispositivi che segnalano un tipo di dispositivo diverso da`"android"`. Tuttavia, la regola non corrisponderà ai dispositivi che non segnalano affatto un tipo di dispositivo.

La gestione delle eccezioni di accesso ai dispositivi mobili

Utilizzi le eccezioni di accesso ai dispositivi mobili per ignorare i risultati delle regole di accesso ai dispositivi mobili. Le sostituzioni si applicano a utenti e dispositivi specifici e annullano la regola di accesso predefinita. Puoi anche utilizzare le sostituzioni per creare eccezioni una tantum alle regole di accesso e consentire o negare specifiche coppie di utenti e dispositivi. Inoltre, puoi utilizzare le sostituzioni con una regola di accesso ai dispositivi mobili. `DefaultDenyAll` Ciò rimanda le decisioni di accesso a una soluzione di gestione dei dispositivi mobili (MDM) di terze parti. Per ulteriori informazioni, consulta Gestione delle eccezioni e Integrazione con soluzioni di gestione dei dispositivi mobili.

Argomenti

Come funzionano le eccezioni relative all'accesso ai dispositivi mobili

Le sostituzioni di accesso ai dispositivi mobili vengono create per una specifica coppia utente/dispositivo. L'override annulla il risultato di accesso predefinito durante la valutazione delle regole di accesso ai dispositivi mobili per un determinato utente e dispositivo. Ad esempio, se una regola di accesso normalmente nega l'accesso, un'eccezione di accesso consente all'utente e al dispositivo di sincronizzare la posta elettronica. Al contrario, se una regola di accesso normalmente consente l'accesso, è possibile creare un'eccezione che impedisca all'utente e al dispositivo di sincronizzare la posta. Quando elimini l'override di accesso a un dispositivo mobile, Amazon rispetta WorkMail nuovamente il risultato delle attuali regole di accesso ai dispositivi mobili quando decide se concedere l'accesso a quell'utente e dispositivo.

> **Important**
>
> Quando modifichi l'override di accesso ai dispositivi mobili per un' WorkMail organizzazione Amazon, i dispositivi interessati possono impiegare cinque minuti per seguire l'override aggiornata.

Gestione delle eccezioni

Le eccezioni di accesso ai dispositivi mobili possono essere create, aggiornate o eliminate utilizzando l'API o. AWS Command Line Interface Per ulteriori informazioni su AWS CLI, consulta la AWS Command Line Interface User Guide.

Per trovare l'ID del dispositivo, usa il AWS Management Console. Per ulteriori informazioni, vedere Visualizzazione dei dettagli del dispositivo mobile.

Elencare le eccezioni di accesso ai dispositivi mobili

Questo esempio mostra come elencare tutte le eccezioni di accesso ai dispositivi mobili per un'organizzazione Amazon WorkMail specificata.

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Creazione e aggiornamento delle eccezioni di accesso ai dispositivi mobili

Ciò creerà un override di accesso ai dispositivi mobili per negare l'accesso all' WorkMailorganizzazione, all'utente e all'ID del dispositivo Amazon specificati.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect DENY
```

Un'eccezione di accesso a un dispositivo mobile esistente può essere modificata per avere un effetto diverso. Ciò aggiornerà l'override di accesso ai dispositivi mobili creato in precedenza per consentire l'accesso anziché negarlo.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect ALLOW
```

L'eliminazione delle regole di accesso ai dispositivi mobili sostituisce le regole di accesso

Ciò eliminerà l'override di accesso ai dispositivi mobili per l' WorkMail organizzazione, l'utente e l'ID del dispositivo Amazon specificati.

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0
```

Integrazione con soluzioni di gestione dei dispositivi mobili

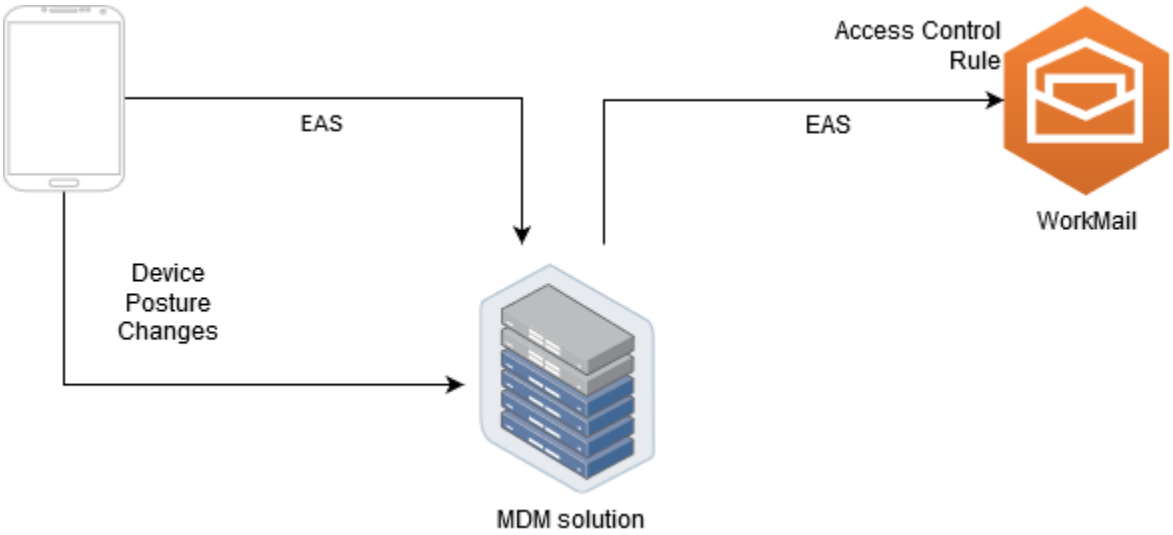
Amazon WorkMail supporta alcune funzionalità di base per la gestione dei dispositivi mobili tramite policy e regole di accesso ai dispositivi mobili. Tuttavia, tali funzionalità possono interagire con i dispositivi mobili solo tramite il protocollo Microsoft Exchange ActiveSync (EAS), quindi hanno una capacità limitata di introspezione e applicazione della posizione di sicurezza dei dispositivi. Gli amministratori che necessitano di un maggiore controllo sulla sicurezza e sulla conformità dei dispositivi possono utilizzare una soluzione di gestione dei dispositivi mobili (MDM) di terze parti.

Panoramica delle soluzioni di gestione dei dispositivi mobili

È possibile configurare la soluzione MDM in due modalità, proxy o diretta. Consultate la documentazione MDM per vedere quali modalità sono supportate dalla vostra soluzione.

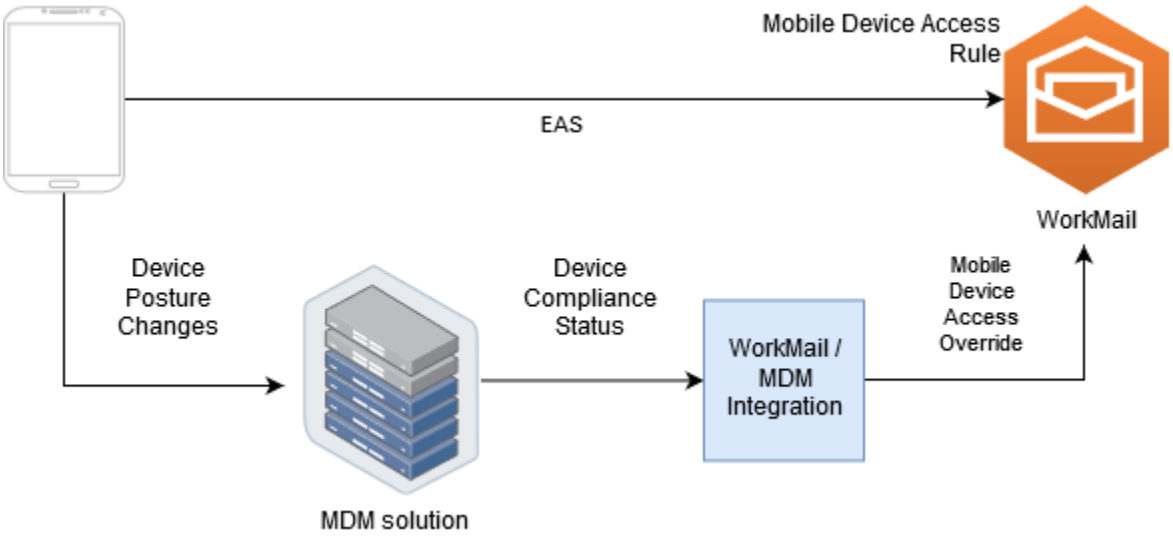
In modalità proxy, i dispositivi mobili utilizzano il protocollo Exchange Active Sync (EAS) tramite la soluzione MDM per accedere ad Amazon WorkMail. La soluzione MDM utilizza la postura del dispositivo per consentire o negare l'accesso ai dati di Amazon. WorkMail Per quanto WorkMail riguarda Amazon, utilizza una regola di controllo degli accessi che consenta l'accesso EAS solo dall'indirizzo o dagli indirizzi IP della soluzione MDM. Per ulteriori informazioni, consulta Lavorare con le regole di controllo degli accessi.

L'immagine seguente mostra una configurazione tipica della modalità proxy.



In modalità diretta, i dispositivi mobili utilizzano EAS per accedere WorkMail direttamente ad Amazon. La tua soluzione MDM riceve le modifiche alla postura del dispositivo e valuta continuamente se ciascun dispositivo soddisfa tali requisiti. Quando la soluzione MDM rileva cambiamenti di postura, ad esempio un dispositivo che non è conforme, può intraprendere diverse azioni e in genere emette notifiche o eventi. Un WorkMail amministratore Amazon può configurare un sistema per ascoltare questi eventi relativi allo stato di conformità e creare automaticamente eccezioni di accesso ai dispositivi mobili che consentono o negano l'accesso ai dispositivi quando entrano o non sono conformi ai requisiti dei dispositivi MDM.

L'immagine seguente mostra una tipica configurazione in modalità diretta.



Configurazione di un' WorkMail organizzazione per l'integrazione con una soluzione MDM di terze parti in modalità diretta

Per l'integrazione con una soluzione di gestione dei dispositivi mobili (MDM) di terze parti in modalità diretta, è necessario soddisfare i seguenti requisiti:

- Crea regole di controllo degli accessi che limitino l'accesso ai dispositivi degli utenti solo al ActiveSync protocollo.
- Crea una regola di accesso ai dispositivi mobili predefinita deny-to-all "" per garantire che tutti i dispositivi mobili sconosciuti o non gestiti vengano negati per impostazione predefinita.
- Adotta una soluzione di gestione dei dispositivi mobili che emetta notifiche o eventi personalizzati quando un dispositivo cambia posizione di sicurezza, vale a dire che entra o non è conforme.
- Crea un componente software personalizzato per ascoltare tali notifiche e chiama Amazon WorkMail SDK per creare eccezioni di accesso ai dispositivi mobili.

Questi componenti assicurano che tutti i dispositivi utente soddisfino i requisiti di conformità MDM prima di poter accedere alle loro caselle di WorkMail posta Amazon.

Utilizza le regole di controllo degli accessi per limitare l'accesso dei dispositivi mobili a ActiveSync

È necessario assicurarsi che tutti i dispositivi utilizzino solo il ActiveSync protocollo e a tale scopo è possibile utilizzare le regole di controllo dell'accesso. Ad esempio, è possibile concedere l'accesso ad altri protocolli di posta solo da un intervallo di indirizzi IP aziendale interno e quindi consentirlo solo ActiveSync quando si accede alla posta elettronica dall'esterno del firewall aziendale. È necessario

eseguire questa operazione perché ActiveSync consente di identificare i dispositivi solo utilizzando un ID dispositivo. Non è possibile utilizzare protocolli come l'Internet Message Access Protocol (IMAP) o i servizi Web di Exchange. Per ulteriori informazioni, consulta Utilizzo delle regole di controllo degli accessi.

Crea una regola di accesso predefinita «nega a tutti»

Per rimandare tutte le decisioni di accesso ai dispositivi mobili alla soluzione di gestione dei dispositivi mobili di terze parti, crea una regola di accesso che neghi automaticamente tutti i dispositivi a meno che non venga sostituita per utente o per dispositivo. Per ulteriori informazioni, vedi Gestione delle regole di accesso ai dispositivi mobili.

Questo esempio mostra una regola «nega a tutti».

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

Reagisci ai cambiamenti di postura del dispositivo e crea eccezioni di accesso ai dispositivi mobili

È necessario configurare la soluzione MDM per inviare notifiche per le modifiche alla postura del dispositivo. Queste notifiche devono essere utilizzate da un componente in grado di utilizzare Amazon WorkMail SDK per creare o aggiornare le eccezioni di accesso ai dispositivi mobili. Per impostazione predefinita, Amazon WorkMail nega l'accesso a dispositivi non gestiti o di nuova fornitura a causa della regola di accesso predefinita «nega a tutti» ai dispositivi mobili mostrata in precedenza in questo argomento. Quando la soluzione MDM stabilisce che il dispositivo soddisfa tutti i requisiti ed emette una notifica che indica che il dispositivo è conforme, questo componente può reagire a questa notifica creando un override di accesso ai dispositivi mobili con effetto per l'utente e il dispositivo specificati. `ALLOW` Se successivamente il dispositivo non è più conforme, la soluzione di gestione dei dispositivi mobili emette un'altra notifica e l'override di accesso può essere eliminata o modificata per negare l'accesso a quel dispositivo. Per ulteriori informazioni, consulta La gestione delle eccezioni di accesso ai dispositivi mobili.

Per un esempio di Amazon WorkMail integrato con MDM, consulta questa applicazione AWS di esempio.

Utilizzo delle autorizzazioni della casella di posta

Puoi utilizzare le autorizzazioni delle cassette postali in Amazon WorkMail per concedere a utenti e gruppi il diritto di lavorare nelle cassette postali di altri utenti. Le autorizzazioni delle cassette postali si applicano a un'intera casella di posta. Consentono a più utenti di accedere alla stessa cassetta postale senza condividere le credenziali di quella cassetta postale. Gli utenti con le autorizzazioni della casella di posta sono in grado di leggere e modificare i dati della casella di posta e di inviare e-mail dalla casella di posta condivisa.

> **Note**
>
> Gli utenti con autorizzazioni per una cassetta postale appartenente a un utente nascosto dall'elenco di indirizzi globale possono comunque accedere alla cassetta postale dell'utente nascosto.

L'elenco seguente mostra le autorizzazioni che puoi concedere:

- Accesso completo: consente l'accesso completo in lettura e scrittura alla cassetta postale, incluse le autorizzazioni per modificare le autorizzazioni a livello di cartella.

  > **Note**
  >
  > Questa opzione è disponibile solo per gli utenti. Ai gruppi non possono essere concessi diritti di accesso completi.

- Invia per conto di un altro utente: consente a un utente o a un gruppo di inviare e-mail per conto di un altro utente. Il proprietario della casella di posta viene visualizzato nell'intestazione From: (Da:) e il mittente appare nell'intestazione Sender: (Mittente:).
- Invia come: consente a un utente o a un gruppo di inviare e-mail come proprietario della cassetta postale, senza mostrare il mittente effettivo del messaggio. Il proprietario della casella di posta viene visualizzato sia nell'intestazione From: (Da:) sia nell'intestazione Sender: (Mittente:).
- Nessuno: impedisce a un utente o a un gruppo di inviare e-mail.

> **Note**
>
> La concessione delle autorizzazioni della casella di posta a un gruppo estende tali autorizzazioni a tutti i membri del gruppo, tra cui i membri dei gruppi nidificati.

Quando concedi le autorizzazioni per le caselle di posta, il WorkMail AutoDiscover servizio Amazon aggiorna automaticamente l'accesso a tali caselle di posta per gli utenti o i gruppi che hai aggiunto.

Per il client Microsoft Outlook in Windows, gli utenti con autorizzazioni di accesso completo possono accedere automaticamente alle caselle di posta condivise. Attendi fino a 60 minuti per la propagazione delle modifiche, quindi riavvia Microsoft Outlook.

Per l'applicazione WorkMail web Amazon e in altri client di posta elettronica, gli utenti con autorizzazioni di accesso complete possono aprire manualmente le caselle di posta condivise. Le caselle di posta aperte restano aperte, anche tra le sessioni, a meno che l'utente non le chiuda.

Argomenti

Informazioni sulle autorizzazioni delle caselle di posta e delle cartelle

Le autorizzazioni delle cassette postali si applicano a tutte le cartelle all'interno di una casella di posta. Queste autorizzazioni possono essere abilitate solo dal titolare dell' AWS account o da un utente IAM autorizzato a chiamare l'API di WorkMail gestione Amazon. Per impostare e modificare le autorizzazioni per le caselle di posta o per i gruppi nel loro insieme, usa AWS Management Console o l'API Amazon WorkMail . È possibile gestire fino a 100 caselle di posta e le autorizzazioni di gruppo dalla console. Per gestire le autorizzazioni per più utenti e gruppi, utilizza l' WorkMail API Amazon.

Le autorizzazioni di cartella si applicano solo a una singola cartella. Gli utenti finali possono impostare le autorizzazioni delle cartelle utilizzando un client di posta elettronica o utilizzando l'applicazione WorkMail web Amazon. Per ulteriori informazioni sull'utilizzo dell'applicazione WorkMail web Amazon per condividere cartelle, consulta Condivisione di cartelle e autorizzazioni per le cartelle nella Amazon WorkMail User Guide.

Gestione delle autorizzazioni delle cassette postali per gli utenti

Puoi utilizzare la WorkMail console Amazon per gestire le autorizzazioni delle caselle di posta per utenti e gruppi. Le seguenti sezioni spiegano come gestire le autorizzazioni per gli utenti. Per informazioni sulla gestione delle autorizzazioni per i gruppi, fare riferimento a. Gestione delle autorizzazioni delle cassette postali per i gruppi

Argomenti

Aggiunta di autorizzazioni

Quando si aggiungono autorizzazioni, si concede a un utente il diritto di eseguire una o più attività nella cassetta postale di un altro utente. Ad esempio, supponiamo che il dipendente A debba inviare messaggi per conto del suo supervisore, il dipendente B. Per concedere tale autorizzazione, si accede alle impostazioni della cassetta postale del dipendente B e si concede al dipendente A il permesso di eseguire l'attività richiesta.

Per aggiungere le autorizzazioni per le cassette postali

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione . Dalla barra di navigazione, scegli la regione che soddisfa le tue esigenze. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione per cui desideri gestire le autorizzazioni.
3. Nel riquadro di navigazione, scegli Utenti, quindi seleziona il nome dell'utente per il quale desideri gestire le autorizzazioni.
4. Selezionare la scheda Permissions (Autorizzazioni) e selezionare Add permissions (Aggiungi autorizzazioni).

   Viene visualizzata la finestra di dialogo Aggiungi autorizzazioni.
5. Apri l'elenco Aggiungi nuove autorizzazioni e seleziona l'utente o il gruppo che deve accedere alla cassetta postale.

6. In Autorizzazioni cassetta postale e Autorizzazioni di invio, scegli le opzioni desiderate.
7. Scegli Aggiungi.

La propagazione delle nuove autorizzazioni agli utenti può richiedere fino a cinque minuti.

Modifica delle autorizzazioni delle cassette postali per gli utenti

Quando si modificano le autorizzazioni della cassetta postale per un utente, si modifica l'accesso che gli altri hanno alla cassetta postale di quell'utente. La modifica delle autorizzazioni della cassetta postale non modifica l'accesso per l'utente originale della cassetta postale.

Per modificare le autorizzazioni della casella di posta

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione . Dalla barra di navigazione, scegli la regione che soddisfa le tue esigenze. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione per cui desideri gestire le autorizzazioni.
3. Nel riquadro di navigazione, scegli Utenti, quindi seleziona il nome dell'utente di cui desideri modificare le autorizzazioni.
4. Scegli la scheda Autorizzazioni.

   Viene visualizzato un elenco degli utenti e dei gruppi che hanno accesso alla cassetta postale.
5. Seleziona il pulsante di opzione accanto all'utente o al gruppo che desideri modificare, quindi esegui una delle seguenti operazioni:

   Per rimuovere le autorizzazioni di un utente

   1. Scegli Rimuovi.

      Viene visualizzata la finestra di dialogo Rimuovi autorizzazioni.
   2. Nella finestra di dialogo Rimuovi autorizzazioni, scegli Rimuovi.

   Per modificare le autorizzazioni di un utente

   1. Scegli Modifica.

Viene visualizzata la finestra di dialogo Modifica autorizzazioni.

2. Imposta le autorizzazioni necessarie, quindi scegli Salva.

Per concedere a un altro utente le autorizzazioni per la cassetta postale

1. Scegli Aggiungi autorizzazioni.

   Viene visualizzata la finestra di dialogo Aggiungi autorizzazioni.
2. Apri l'elenco Aggiungi nuove autorizzazioni e seleziona l'utente che desideri aggiungere.
3. Imposta le autorizzazioni necessarie, quindi scegli Aggiungi.

La propagazione delle modifiche alle autorizzazioni agli utenti può richiedere fino a cinque minuti.

Gestione delle autorizzazioni delle cassette postali per i gruppi

Puoi aggiungere o rimuovere le autorizzazioni di gruppo per Amazon WorkMail.

> **Note**
>
> Non puoi applicare le autorizzazioni di accesso completo a un gruppo, perché i gruppi non dispongono di una casella di posta a cui accedere.

Per gestire le autorizzazioni di gruppo

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modifica l'opzione Regione AWS Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione per cui desideri gestire le autorizzazioni.
3. Nel riquadro di navigazione, scegli Gruppi, quindi seleziona il nome del gruppo per il quale desideri impostare le autorizzazioni.
4. Scegli la scheda Autorizzazioni, quindi scegli Aggiungi autorizzazioni.

Viene visualizzata la finestra di dialogo Aggiungi autorizzazioni.

5. Apri l'elenco Aggiungi nuove autorizzazioni e seleziona l'utente o il gruppo a cui concedere le autorizzazioni per la cassetta postale.
6. In Autorizzazioni cassetta postale e Autorizzazioni di invio, scegli le opzioni desiderate.
7. Scegli Aggiungi.

La propagazione delle modifiche alle autorizzazioni agli utenti può richiedere fino a cinque minuti.

Accesso programmatico alle caselle di posta

Per accedere in modo programmatico alle WorkMail caselle di posta Amazon, utilizza il protocollo Exchange Web Services (EWS). Con EWS, puoi accedere a tutti i tipi di elementi in una casella di posta. Ecco alcune librerie EWS che puoi usare con Amazon WorkMail:

- Java — API Java EWS
- .Net — API gestita da EWS
- Python — Exchangelib

Amazon supporta WorkMail anche i protocolli IMAP e SMTP, che puoi utilizzare per inviare e ricevere e-mail. Puoi vedere i WorkMail protocolli URLs supportati per Amazon nella sezione WorkMailEndpoint e quote Amazon.

Quando si utilizza il protocollo EWS, Amazon WorkMail supporta i seguenti metodi di autenticazione:

- Autenticazione di base: con l'autenticazione di base, inserisci un indirizzo e-mail e una password.
- Ruoli di impersonificazione: con i ruoli di impersonificazione, accedi alle cassette postali degli utenti senza inserire le credenziali dell'utente.

Argomenti

Gestione dei ruoli di impersonificazione

Con i ruoli di impersonificazione, gli amministratori configurano l'accesso programmatico alle cassette postali degli utenti senza inserire le credenziali dell'utente. I servizi e gli strumenti possono assumere un ruolo di impersonificazione per eseguire azioni nelle caselle di posta degli utenti. L'impersonificazione è supportata solo con il protocollo EWS.

Panoramica dei ruoli di impersonificazione

Per consentire l'impersonificazione, gli amministratori devono creare un ruolo di impersonificazione con le seguenti proprietà:

- Tipo di ruolo: scegli Accesso completo o Sola lettura. Il tipo di ruolo limita il tipo di operazioni che un ruolo può eseguire.
- Regole: un elenco di regole che definiscono gli utenti che il ruolo di impersonificazione può impersonare.

Amazon WorkMail valuta le regole in base alle seguenti condizioni:

- Se una delle regole DENY corrisponde, la policy nega l'impersonificazione. Le regole DENY hanno la precedenza su qualsiasi regola ALLOW.
- Se almeno una regola ALLOW corrisponde e nessuna regola DENY corrisponde, la politica consente l'impersonificazione.
- Se non si applica alcuna regola, l'impersonificazione viene negata.

> **Note**
>
> Per consentire l'impersonificazione per tutti gli utenti di WorkMail un'organizzazione Amazon, crea una regola con l'effetto ALLOW e senza condizioni.

> **Warning**
>
> Devi creare regole per consentire a un ruolo di impersonificazione di impersonare un utente. Se non si specificano regole, un ruolo di impersonificazione non può assumere i diritti di accesso di un utente.

Dopo aver creato il ruolo di impersonificazione, puoi utilizzarlo per accedere alle cassette postali degli utenti. Per ulteriori informazioni, consulta Utilizzo dei ruoli di impersonificazione.

Considerazioni relative alla sicurezza

L'uso di ruoli di impersonificazione crea potenziali problemi di sicurezza all'interno della tua WorkMail organizzazione Amazon e. Account AWS Ecco alcuni dei potenziali problemi da considerare quando si crea un ruolo di impersonificazione:

- Autorizzazioni transitive: se l'utente A ha accesso alla cassetta postale dell'utente B e un ruolo di impersonificazione può impersonare l'utente A, questo ruolo di impersonificazione può impersonare le autorizzazioni di accesso dell'utente A e accedere alla cassetta postale B dell'utente.
- Controllo degli accessi: è possibile utilizzare le regole di controllo degli accessi per limitare l'accesso al ruolo di impersonificazione. Per ulteriori informazioni, consulta Utilizzo delle regole di controllo degli accessi.
- Policy IAM: puoi assegnare un'`AssumeImpersonationRole`azione a una particolare WorkMail organizzazione Amazon e a un ruolo di impersonificazione utilizzando la condizione. `workmail:ImpersonationRoleId` Per vedere un esempio di policy IAM, consulta. Come WorkMail funziona Amazon con IAM

Creazione di ruoli di imitazione

Puoi creare ruoli di impersonificazione dalla console Amazon WorkMail .

Per creare un ruolo di imitazione

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione . Dalla barra di navigazione, scegli la regione che soddisfa le tue esigenze. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione.
3. Scegli Ruoli di impersonificazione, quindi scegli Crea ruolo.
4. Viene visualizzata la finestra di dialogo Crea ruolo di impersonificazione. In Ruolo, inserisci le seguenti informazioni:
   - Nome: inserisci un nome univoco per il ruolo di impersonificazione.
   - (Facoltativo) Descrizione: inserisci una descrizione per il ruolo di impersonificazione.
   - Tipo di ruolo: scegli Sola lettura o Accesso completo.
5. In Regole, scegli Aggiungi regola.
6. Viene visualizzata la finestra di dialogo Aggiungi regola. Immetti le seguenti informazioni:
   - Nome: immettere un nome univoco per la regola.
   - (Facoltativo) Descrizione: immettere una descrizione per la regola.

- In Effetto, scegli Consenti o Nega. Ciò consente o nega l'accesso in base alle condizioni selezionate nel passaggio successivo.
- (Facoltativo) In base a questa regola:, scegli Corrisponde alle richieste che impersonano gli utenti selezionati per includere utenti specifici. Scegli Corrisponde alle richieste che impersonano utenti diversi dagli utenti selezionati per aggiungere utenti diversi dagli utenti selezionati.

7. Scegli Aggiungi regola.

> **Note**
>
> Le regole vengono salvate solo quando si salva il ruolo corrispondente.

8. Scegliere Crea ruolo.

Modifica dei ruoli di impersonificazione

Puoi modificare i ruoli di impersonificazione dalla console Amazon WorkMail .

Per modificare un ruolo di impersonificazione

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione . Dalla barra di navigazione, scegli la regione che soddisfa le tue esigenze. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione.
3. Scegli Ruoli di impersonificazione.
4. Seleziona il nome del ruolo di impersonificazione che desideri modificare, quindi scegli Modifica.
5. Viene visualizzata la finestra di dialogo Modifica ruolo di rappresentazione. In Ruolo, inserisci le seguenti informazioni:

   - Nome: inserisci un nome univoco per il ruolo di impersonificazione.
   - (Facoltativo) Descrizione: inserisci una descrizione per il ruolo di impersonificazione.
   - Tipo di ruolo: per concedere al ruolo di impersonificazione l'accesso in sola lettura alla cassetta postale di un utente, scegli Sola lettura. Per concedere al ruolo di impersonificazione

i diritti di lettura e modifica degli elementi nella cassetta postale di un utente, scegli Accesso completo.

6. In Regole, seleziona la regola che desideri modificare e scegli Modifica.
7. Viene visualizzata la finestra di dialogo Modifica regola. Immetti le seguenti informazioni:
   - Nome: modifica il nome della regola.
   - (Facoltativo) Descrizione: aggiorna o inserisci una descrizione per la regola.
   - In Effetto, scegli Consenti per consentire l'accesso quando vengono soddisfatte le condizioni impostate nelle regole. Per negare l'accesso, scegli Nega.
   - (Facoltativo) In base a questa regola:, scegli Corrisponde alle richieste che si spacciano per gli utenti selezionati per includere utenti specifici. Scegli Corrisponde alle richieste che impersonano utenti diversi dagli utenti selezionati per aggiungere utenti diversi dagli utenti selezionati.
8. Seleziona Salva.
9. Scegli Save changes (Salva modifiche).

> **Important**
>
> Quando modifichi una regola di impersonificazione, l'aggiornamento delle cassette postali interessate può richiedere fino a cinque minuti. Durante il processo di aggiornamento delle regole, è possibile che si verifichino comportamenti incoerenti nella cassetta postale. Tuttavia, se provi un ruolo, Amazon WorkMail risponde come previsto in base alla regola aggiornata. Per ulteriori informazioni, consulta Test dei ruoli di impersonificazione.

Test dei ruoli di impersonificazione

Puoi testare un ruolo di impersonificazione dalla console Amazon WorkMail .

Per testare un ruolo di impersonificazione

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione . Dalla barra di navigazione, scegli la regione che soddisfa le tue esigenze. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.

2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione.
3. Scegli Ruoli di impersonificazione.
4. Seleziona il ruolo di impersonificazione che desideri testare.
5. Scegli il ruolo di test.
6. Viene visualizzata la finestra di dialogo Test impersonation role. In Utente Target, seleziona l'utente per il quale desideri testare l'accesso all'impersonificazione.
7. Scegli Test (Esegui test).

Eliminazione dei ruoli di impersonificazione

Puoi eliminare un ruolo di impersonificazione dalla console Amazon WorkMail .

Per eliminare un ruolo di impersonificazione

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, modificare la regione . Dalla barra di navigazione, scegli la regione che soddisfa le tue esigenze. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome dell'organizzazione.
3. Scegli Ruoli di impersonificazione.
4. Seleziona il nome del ruolo di impersonificazione che desideri eliminare.
5. Scegli Elimina.
6. Viene visualizzata la finestra di dialogo Elimina ruolo. Per confermare l'eliminazione, inserite il nome del ruolo nella finestra di dialogo e scegliete Elimina.

Utilizzo dei ruoli di impersonificazione

Per accedere ai dati delle cassette postali, utilizza l'azione `AssumeImpersonationRole` Amazon WorkMail API. Per maggiori dettagli su Amazon WorkMail APIs, consulta API Reference.

`AssumeImpersonationRole`restituisce un`Token`. Questo `Token` deve essere passato entro 15 minuti al protocollo EWS tramite l'`Authorization`intestazione HTTP.

Gli esempi seguenti mostrano come utilizzare i ruoli di impersonificazione con il protocollo EWS. Le costanti utilizzate negli esempi specificano i seguenti dettagli esclusivi dell'organizzazione e dell'account:

- *WORKMAIL_ORGANIZATION_ID*— ID WorkMail dell'organizzazione Amazon
- *IMPERSONATION_ROLE_ID*— ID del ruolo di impersonificazione
- *WORKMAIL_EWS_URL*— Endpoint EWS disponibile presso gli endpoint e le quote di Amazon WorkMail
- *EMAIL_ADDRESS*— Indirizzo e-mail della casella di posta dell'utente

Example Java — API Java EWS

```
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 — API gestita da EWS

```
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
)
```

Esportazione del contenuto delle cassette postali

Utilizza l'azione StartMailboxExportJobAPI in Amazon WorkMail API Reference per esportare il contenuto delle caselle di WorkMail posta Amazon in un bucket Amazon Simple Storage Service (Amazon S3). Questa azione esporta tutti i messaggi e-mail e gli elementi del calendario dalla casella di posta specificata in un `.zip` file nel bucket Amazon S3, in formato MIME. Gli altri elementi, come contatti e attività, non vengono esportati.

Il tempo necessario per il completamento del processo di esportazione della cassetta postale dipende dalle dimensioni e dal numero di elementi nella cassetta postale. Poiché il processo di esportazione della cassetta postale avviene in un determinato periodo di tempo, non rappresenta un'istantanea del contenuto della cassetta postale in un singolo momento. Per visualizzare lo stato di un processo di esportazione, utilizza le azioni DescribeMailboxExportJobo ListMailboxExportJobsAPI in Amazon WorkMail API Reference.

Quando un processo di esportazione di una casella di posta viene completato, il `.zip` file nel bucket Amazon S3 viene crittografato utilizzando la chiave master del cliente (CMK) AWS Key Management Service symmetric AWS KMS() fornita. Poiché AWS KMS la crittografia è integrata con Amazon S3, i dati decrittografati sono visibili all'utente che li scarica, purché l'utente abbia accesso alla CMK. AWS KMS

Prerequisiti

Di seguito sono riportati i prerequisiti per l'esportazione del contenuto delle cassette postali:

- La capacità di programmare.
- Un account WorkMail amministratore Amazon.
- Un bucket Amazon S3 che non consente l'accesso pubblico. Per ulteriori informazioni, consulta Using Amazon S3 block public access nella Amazon Simple Storage Service User Guide e nella Amazon Simple Storage Service User Guide.
- Una CMK simmetrica AWS KMS . Per ulteriori informazioni, consulta l'argomento relativo alle nozioni di base nella Guida per gli sviluppatori di AWS Key Management Service .
- Un ruolo AWS Identity and Access Management (IAM) con una policy che concede l'autorizzazione a scrivere nel bucket Amazon S3 e crittografare i file inviati con CMK. AWS KMS Per ulteriori informazioni, consulta Come WorkMail funziona Amazon con IAM.

Esempi di policy IAM e creazione di ruoli

L'esempio seguente mostra una policy IAM che concede l'autorizzazione a scrivere nel bucket Amazon S3 e crittografare i file inviati con CMK. AWS KMS Per utilizzare questa policy di esempio nella Esempio: esportazione del contenuto delle cassette postali procedura seguente, salva la policy come file JSON con nome di file. `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*"
                }
            }
        }
    ]
```

```
}
```

L'esempio seguente mostra una policy di fiducia IAM allegata al ruolo IAM che crei. Per utilizzare questa policy di esempio nella Esempio: esportazione del contenuto delle cassette postali procedura seguente, salvate la policy come file JSON con nome `mailbox-export-trust-policy.json` di file.

Non è necessario utilizzare le `aws:SourceAccount` condizioni `aws:SourceArn` and contemporaneamente. Ad esempio, puoi rimuovere `aws:SourceArn` dalla policy se devi utilizzare lo stesso ruolo per esportare messaggi da diverse WorkMail organizzazioni Amazon con lo stesso AWS account. Per ulteriori informazioni sulle chiavi di condizione, consulta le chiavi di contesto delle condizioni AWS globali nella guida per l'utente di AWS Identity and Access Management.

```
{
  "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"
        }
      }
    }
  ]
}
```

Puoi utilizzare il AWS CLI per creare il ruolo IAM nel tuo account eseguendo i seguenti comandi.

```
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
```

Per ulteriori informazioni su AWS CLI, consulta la Guida AWS Command Line Interface per l'utente.

Esempio: esportazione del contenuto delle cassette postali

Dopo aver creato il ruolo e le policy IAM nella sezione precedente, completa i seguenti passaggi per esportare il contenuto della tua casella di posta. Devi disporre WorkMail dell'ID dell'organizzazione Amazon e dell'ID utente (ID entità), a cui puoi accedere nella WorkMail console Amazon o utilizzando l' WorkMail API Amazon.

Esempio: per esportare il contenuto della casella di posta

1. Utilizzare il AWS CLI per avviare il processo di esportazione delle cassette postali.

   ```
   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. Utilizza AWS CLI per monitorare lo stato dei processi di esportazione delle caselle di posta per la tua WorkMail organizzazione Amazon.

   ```
   aws workmail list-mailbox-export-jobs --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56
   ```

   In alternativa, utilizza l'ID del lavoro generato dal **`start-mailbox-export-job`** comando per monitorare solo lo stato del processo di esportazione della casella di posta.

   ```
   aws workmail describe-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
   ```

Quando lo stato del processo di esportazione della cassetta postale è COMPLETATO, gli elementi della cassetta postale esportati sono disponibili in un `.zip` file nel bucket Amazon S3 specificato.

Di seguito è riportato un esempio del log di output dalla casella di posta esportata:

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportableGli elementi non sono supportati come note e contatti.

Considerazioni

Le seguenti considerazioni si applicano all'esportazione dei lavori relativi alle caselle di posta per Amazon: WorkMail

- Puoi eseguire fino a 10 processi di esportazione simultanei di caselle di posta per una determinata organizzazione Amazon WorkMail .
- Puoi eseguire un processo di esportazione delle caselle di posta per una determinata casella di posta anche una volta ogni 24 ore.
- Le seguenti risorse devono trovarsi tutte nella stessa AWS regione:
  - WorkMail Organizzazione Amazon
  - AWS KMS CMK
  - Bucket Amazon S3

Risoluzione dei problemi

Gli argomenti di questa sezione spiegano come risolvere i problemi in Amazon. WorkMail

Argomenti

Visualizzazione delle intestazioni di posta elettronica

Le informazioni contenute nelle intestazioni delle e-mail possono aiutarti a risolvere i problemi più comuni relativi alle e-mail degli utenti. Amazon ti WorkMail consente di visualizzare le informazioni di intestazione di qualsiasi messaggio.

Per visualizzare le intestazioni delle e-mail in Amazon WorkMail

1. Nell'applicazione WorkMail web Amazon, fai doppio clic sul messaggio e-mail per aprirlo.
2. Scegli le opzioni del messaggio (l'icona a forma di ingranaggio e busta) nell'angolo in alto a destra del messaggio, accanto alla data di invio.

Le intestazioni e-mail vengono visualizzate in Intestazioni Internet.

Routing della posta

Se un utente smette di ricevere e-mail, è possibile che la tua WorkMail organizzazione Amazon stia riscontrando un problema di routing della posta. I passaggi di questa sezione spiegano i modi più comuni per risolvere i problemi di consegna e routing.

Problemi relativi alla posta in entrata:

- Controlla il record MX per il dominio associato alla tua WorkMail organizzazione Amazon. `WorkMail`dovrebbe essere l'unica voce e dovrebbe avere la priorità più bassa. La presenza di più record MX può causare la ricezione di messaggi da parte del servizio sbagliato. Per ulteriori informazioni sui record MX, vedereVerifica dei domini.
- Controlla le impostazioni DMARC (Domain-based Message Authentication, Reporting and Conformance) per la tua organizzazione nella console Amazon. WorkMail I record DMARC

vengono utilizzati per proteggere da attacchi comuni, come lo spoofing o il phishing, che possono compromettere le credenziali dell'account di un utente. Per ulteriori informazioni su DMARC, vedere. Applicare le policy DMARC alla posta in entrata

- Controlla la regola di entrata di Amazon Simple Email Service. Se la regola contiene azioni diverse da Amazon WorkMail, tali azioni possono avere esito negativo e causare l'interruzione della ricezione della posta WorkMail da parte di Amazon. Per ulteriori informazioni sulle regole di Amazon SES, consulta l' WorkMail azione Integrate with Amazon nella Amazon Simple Email Service Developer Guide.
- Abilita il tracciamento dei messaggi in Amazon WorkMail, quindi controlla i log per eventuali problemi di consegna. Per ulteriori informazioni sul tracciamento dei messaggi, consultaAbilitazione della registrazione degli eventi via e-mail.

Problemi relativi alla posta in uscita

- Assicurati che il tuo record SPF includa Amazon SES. Controlla la pagina dei domini nella WorkMail console Amazon per verificare. Per ulteriori informazioni su SPF, consulta. Autenticazione delle e-mail con SPF
- Assicurati che Amazon WorkMail disponga delle autorizzazioni per utilizzare il dominio. In caso contrario, aggiungi nuovamente il dominio. Aggiunta di un dominioin questa guida vengono fornite le istruzioni da seguire.

Usare l'e-mail journaling con Amazon WorkMail

È possibile configurare lo storico per registrare la comunicazione per e-mail con l'utilizzo dell'archiviazione di terze parti e di strumenti di eDiscovery. In questo modo vengono rispettate le normative di conformità per la protezione della privacy, storage dei dati e informazioni di protezione.

Utilizzo del journaling

Amazon WorkMail registra tutti i messaggi e-mail inviati a qualsiasi utente dell'organizzazione specificata, nonché tutti i messaggi e-mail inviati dagli utenti di quell'organizzazione. Una copia di tutti i messaggi e-mail viene inviata a un indirizzo specificato dall'amministratore di sistema, in un formato chiamato. `journal record` Questo formato è compatibile con i programmi per e-mail di Microsoft. Il journaling delle-mail non comporta costi aggiuntivi.

Per l'inserimento nel journal vengono utilizzati due indirizzi e-mail: un indirizzo e-mail di inserimento nel journal e un indirizzo e-mail di report. L'indirizzo e-mail per il journaling è l'indirizzo di una casella di posta dedicata, oppure di un dispositivo di terze parti integrato con l'account, al quale vengono inviati i report del journal. L'indirizzo e-mail per il report è l'indirizzo dell'amministratore di sistema, al quale vengono inviate le notifiche dei report di journaling non riusciti.

Tutti i record del journal vengono inviati da un indirizzo e-mail che viene aggiunto automaticamente al dominio e ha l'aspetto seguente.

```
amazonjournaling@yourorganization.awsapps.com
```

Non esiste alcuna casella di posta associata a questo indirizzo e non potrai crearne una utilizzando questo nome o indirizzo.

> **Note**
>
> non eliminare il seguente record di dominio dalla console Amazon Simple Email Service (Amazon SES), altrimenti l'email journaling smetterà di funzionare.
>
> ```
> yourorganization.awsapps.com
> ```

Ogni messaggio e-mail in entrata o in uscita genera un record di diario, indipendentemente dal numero di destinatari o gruppi di utenti. Le e-mail incapaci di generare un report di journaling generano una notifica di errore, che viene inviata all'indirizzo e-mail per il report.

Per abilitare il journaling delle e-mail

1. Apri la WorkMail console Amazon all'indirizzo https://console.aws.amazon.com/workmail/.

   Se necessario, cambia la AWS regione. Nella barra nella parte superiore della finestra della console, apri l'elenco Seleziona una regione e scegli una regione. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint nella Riferimenti generali di Amazon Web Services.
2. Nel riquadro di navigazione, scegli Organizations, quindi scegli il nome della tua organizzazione.
3. Nel riquadro di navigazione, Impostazioni dell'organizzazione, scegli la scheda Journaling, quindi scegli Modifica.
4. Sposta il cursore di stato di Journaling in posizione On.
5. nella casella Indirizzo e-mail di Journaling, inserite l'indirizzo e-mail fornito dal provider di e-mail journaling.

   > **Note**
   >
   > Ti consigliamo di usare un provider dedicato per il journaling.
6. Nella casella Indirizzo e-mail del report, inserisci l'indirizzo dell'amministratore di posta elettronica.
7. Seleziona Salva. Le modifiche vengono applicate immediatamente.

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti in ogni versione dell'Amazon WorkMail Administrator Guide. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile sottoscrivere un feed RSS.

Modifica	Descrizione	Data
Supporto per la registrazione degli audit	I registri di controllo possono essere utilizzati per monitorare l'accesso degli utenti alle caselle di posta, verificare la presenza di attività sospette ed eseguire il debug del controllo degli accessi e delle configurazioni dei provider di disponibilità. Per ulteriori informazioni, consulta Enabling audit logging e Logging and monitoring in Amazon WorkMail nella Amazon WorkMail Administrator Guide.	20 marzo 2024
Supporto Transport Layer Security (TLS)	Amazon WorkMail ha interrotto il supporto per Transport Layer Security (TLS) 1.0 e 1.1. Se utilizzi TLS 1.0 o 1.1, devi aggiornare la versione TLS alla 1.2.	2 novembre 2023
Utenti remoti	Gli utenti remoti sono WorkMail utenti Amazon ospitati all'esterno dell' WorkMail organizzazione Amazon o ospitati su un dominio di posta elettronica	18 settembre 2023

	diverso. Per ulteriori informazioni, consulta Users in the Amazon WorkMail Administrator Guide.	
Accesso programmatico alle caselle di posta	Amazon offre WorkMail ora i ruoli di impersonificazione per concedere l'accesso programmatico alle caselle di posta. Per ulteriori informazioni, consulta la sezione Accesso programmatico alle caselle di posta nella Amazon WorkMail Administrator Guide.	4 ottobre 2022
Configura fornitori di disponibilità personalizzati su Amazon WorkMail	Amazon WorkMail supporta l'uso di fornitori di disponibilità personalizzati ()CAPs. Per ulteriori informazioni, consulta Configurazione di un provider di disponibilità personalizzato nella Amazon WorkMail Administrator Guide.	30 giugno 2022
Modifiche alla console per la creazione di un'organizzazione	L'esperienza della WorkMail console Amazon per la creazione di un'organizzazione è stata aggiornata. Per ulteriori informazioni, consulta Creating an organization nella Amazon WorkMail Administrator Guide.	23 ottobre 2020

Esportazione del contenuto delle caselle di posta	Utilizza l'azione `StartMailboxExportJob` API per esportare i contenuti delle caselle di WorkMail posta Amazon in un bucket Amazon Simple Storage Service (Amazon S3). Per ulteriori informazioni, consulta Esportazione del contenuto delle cassette postali nella Amazon WorkMail Administrator Guide.	22 settembre 2020
Politiche di conservazione delle caselle di posta	Imposta politiche di conservazione delle caselle di posta per la tua WorkMail organizzazione Amazon che eliminino automaticamente i messaggi e-mail dopo un periodo di tempo a tua scelta. Per ulteriori informazioni, consulta la sezione Impostazione delle politiche di conservazione delle cassette postali nella Amazon WorkMail Administrator Guide.	28 maggio 2020

Azioni Esegui Lambda sincrone e asincrone	Scegli configurazioni sincrone o asincrone per le azioni Esegui Lambda nelle regole del flusso di posta elettroni ca di Amazon. WorkMail Per ulteriori informazioni, consulta la sezione Configurazione AWS Lambda per Amazon WorkMail nella Amazon WorkMail Administrator Guide.	11 maggio 2020
Utilizzo delle regole di controllo degli accessi	Le regole di controllo degli accessi consentono WorkMail agli amministratori di Amazon di controllare l'accesso alle caselle di posta della propria organizzazione. Per ulteriori informazioni, consulta Working with access control rules nella Amazon WorkMail Administr ator Guide.	12 febbraio 2020
Taggare un'organizzazione	Etichetta un' WorkMail organizzazione Amazon per distinguere le organizzazioni nella AWS Billing and Cost Management console o per controllare l'accesso alle risorse dell'organizzazion e. Per ulteriori informazioni, consulta Tagging an organizat ion nella Amazon WorkMail Administrator Guide.	23 gennaio 2020

Applica le politiche DMARC alle e-mail in arrivo	Per ulteriori informazioni, consulta la sezione Applicazione delle politiche DMARC alle e-mail in arrivo nella Amazon WorkMail Administrator Guide.	17 ottobre 2019
Recupero del contenuto dei messaggi con Lambda	Usa l'API Amazon WorkMail Message Flow con AWS Lambda per recuperare il contenuto dei messaggi. Per ulteriori informazioni, consulta Recupero del contenuto dei messaggi con Lambda nella Amazon WorkMail Administrator Guide.	12 settembre 2019
Registrazione degli eventi WorkMail e-mail di Amazon	Abilita la registrazione degli eventi e-mail nella WorkMail console Amazon per tenere traccia dei messaggi e-mail per la tua organizzazione. Per ulteriori informazioni, consulta Tracciamento dei messaggi nella Amazon WorkMail Administrator Guide.	13 maggio 2019
Inserimento di record DNS Route 53	Quando configuri un dominio gestito in una zona ospitata pubblica su Route 53, Amazon inserisce WorkMail automaticamente i record DNS per te. Per ulteriori informazioni, consulta Aggiungere un dominio nella Amazon WorkMail Administrator Guide.	13 febbraio 2019

Configurazione di Lambda per le azioni delle regole di posta elettronica in entrata	Amazon WorkMail supporta la configurazione delle funzioni Lambda da utilizzare con le regole del flusso di posta elettronica in entrata. Per ulteriori informazioni, consulta la sezione Gestione dei flussi di posta elettronica nella Amazon WorkMail Administrator Guide.	24 gennaio 2019
Configurazione di Lambda per Amazon WorkMail	Amazon WorkMail supporta la configurazione delle funzioni Lambda da utilizzare con le regole del flusso di posta elettronica in uscita. Per ulteriori informazioni, consulta Configuring Lambda for Amazon nella WorkMail WorkMail Amazon Administrator Guide.	19 novembre 2018
Routing SMTP	Amazon WorkMail supporta la configurazione di gateway SMTP da utilizzare con le regole del flusso di posta elettronica in uscita. Per ulteriori informazioni, consulta la sezione Configurazione dei gateway SMTP nella Amazon WorkMail Administrator Guide.	1° novembre 2018

Strumenti di debug per domini personalizzati	Amazon WorkMail ha aggiunto strumenti di debug per domini personalizzati. Per ulteriori informazioni, consulta Aggiungere un dominio nella Amazon WorkMail Administrator Guide.	15 ottobre 2018
Support per Outlook 2019	Amazon WorkMail supporta Outlook 2019 per Windows e macOS. Per ulteriori informazioni, consulta i requisiti di WorkMail sistema di Amazon nella Amazon WorkMail Administrator Guide.	1 ottobre 2018
Vari aggiornamenti	Vari aggiornamenti per il layout e l'organizzazione dell'argomento.	12 luglio 2018
Autorizzazioni per le cassette postali	Puoi utilizzare le autorizzazioni delle cassette postali in Amazon WorkMail per concedere a utenti o gruppi il diritto di lavorare nelle cassette postali di altri utenti. Per ulteriori informazioni, consulta Lavorare con le autorizzazioni delle cassette postali nella Amazon WorkMail Administrator Guide.	9 aprile 2018

Support per AWS CloudTrail	Amazon WorkMail è integrato con AWS CloudTrail. Per ulteriori informazioni, consulta la sezione Registrazione delle chiamate WorkMail API Amazon AWS CloudTrail nella Amazon WorkMail Administrator Guide.	12 dicembre 2017
Support per i flussi di posta elettronica	È possibile impostare delle regole per il flusso di e-mail per la gestione delle e-mail in entrata in base all'indirizzo e-mail o al dominio del mittente. Per ulteriori informazioni, consulta la sezione Gestione dei flussi di posta elettronica nella Amazon WorkMail Administrator Guide.	5 luglio 2017
Aggiornamenti a Quick Setup	Quick Setup ora crea una WorkMail directory Amazon per te. Per ulteriori informazioni, consulta Configurare Amazon WorkMail con Quick Setup nella Amazon WorkMail Administrator Guide.	10 maggio 2017
Support per una gamma più ampia di client di posta elettronica	Ora puoi usare Amazon WorkMail con Microsoft Outlook 2016 per Mac e client di posta elettronica IMAP. Per ulteriori informazioni, consulta i requisiti di sistema per Amazon WorkMail nella Amazon WorkMail Administrator Guide.	9 gennaio 2017

Support per il journaling SMTP	È possibile impostare il journaling per la registrazione delle comunicazioni per e-mail. Per ulteriori informazioni, consulta Using email journaling with Amazon WorkMail nella Amazon WorkMail Administrator Guide.	25 Novembre 2016
Support per il reindirizzamento delle e-mail a indirizzi e-mail esterni	Puoi configurare le regole di reindirizzamento delle e-mail aggiornando la policy di identità di Amazon SES per il tuo dominio. Per ulteriori informazioni, consulta Modifica le politiche di identità del dominio nella Amazon WorkMail Administrator Guide.	26 ottobre 2016
Support per l'interoperabilità	Puoi abilitare l'interoperabilità tra Amazon e WorkMail Microsoft Exchange. Per ulteriori informazioni, consulta Interoperabilità tra Amazon e WorkMail Microsoft Exchange nella Amazon WorkMail Administrator Guide.	25 ottobre 2016
Disponibilità generale	La versione di disponibilità generale di Amazon WorkMail.	4 gennaio 2016

Support per la prenotazione delle risorse	Supporto per la prenotazione di risorse, come sale riunioni e attrezzature. Per ulteriori informazioni, consulta Lavorare con le risorse nella Amazon WorkMail Administrator Guide.	19 ottobre 2015
Support per lo strumento di migrazione della posta elettronica	Supporto per lo strumento per la migrazione delle e-mail. Per ulteriori informazioni, consulta la sezione Migrazione ad Amazon WorkMail nella Amazon WorkMail Administrator Guide.	16 agosto 2015
Versione di anteprima di Amazon WorkMail	La versione di anteprima di Amazon WorkMail.	28 gennaio 2015

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.