aws

Guía del administrador

Amazon WorkMail

Version 1.0

Amazon WorkMail: Guía del administrador

Table of Contents

¿Qué es Amazon WorkMail?

Amazon WorkMail es un servicio de correo electrónico y calendario empresarial seguro y gestionado que admite los clientes de correo electrónico móviles y de escritorio existentes. WorkMail Los usuarios de Amazon pueden acceder a su correo electrónico, contactos y calendarios mediante Microsoft Outlook, su navegador o sus aplicaciones de correo electrónico nativas de iOS y Android. Puedes integrar Amazon WorkMail con tu directorio corporativo existente y controlar tanto las claves que cifran tus datos como la ubicación en la que se almacenan.

Para obtener una lista de regiones y puntos de enlace compatibles de AWS, consulte Regiones y puntos de enlace de AWS.

Temas

Requisitos WorkMail del sistema de Amazon

Cuando el WorkMail administrador de Amazon te invite a iniciar sesión en tu WorkMail cuenta de Amazon, podrás iniciar sesión con el cliente WorkMail web de Amazon.

Amazon WorkMail también funciona con los principales dispositivos móviles y sistemas operativos compatibles con el ActiveSync protocolo Exchange. Estos dispositivos incluyen iPad, iPhone, Android y Windows Phone. Los usuarios de macOS pueden añadir su WorkMail cuenta de Amazon a sus aplicaciones de correo, calendario y contactos.

Amazon WorkMail es compatible con las siguientes versiones de sistemas operativos:

- Windows: Windows 7 SP1 o posterior
- macOS: macOS 10.12 (Sierra) o posterior
- Android: Android 5.0 o posterior
- iPhone: iOS 5 o posterior
- Windows phone: Windows 8.1 o posterior

- Blackberry: Blackberry OS 10.3.3.3216

Si tienes una licencia de Microsoft Outlook válida, puedes acceder a Amazon WorkMail con las siguientes versiones de Microsoft Outlook:

- Outlook 2013 o posterior
- Outlook 2013 Click-to-Run o posterior
- Outlook para Mac 2016 o posterior

Puede acceder al cliente WorkMail web de Amazon mediante las siguientes versiones de navegador:

- Google Chrome: versión 2.2 o posterior
- Mozilla Firefox: versión 27 o posterior
- Safari: versión 7 o posterior
- Internet Explorer: versión 11
- Microsoft Edge

También puedes usar Amazon WorkMail con tu cliente IMAP preferido.

WorkMail Conceptos de Amazon

La terminología y los conceptos fundamentales para tu comprensión y uso de Amazon WorkMail se describen a continuación.

Organización

Una configuración de inquilinos para Amazon WorkMail.

Alias

Un nombre exclusivo para identificar una organización. El alias se utiliza para acceder a la aplicación WorkMail web de Amazon (https://*alias*.awsapps.com/mail).

Dominio

La dirección web que aparece después del símbolo @ en una dirección de correo electrónico. Puede añadir un dominio que recibe correo y lo entrega a los buzones de correo de su organización.

Dominio de correo electrónico de prueba

Durante la configuración, se configura automáticamente un dominio que se puede utilizar para probar Amazon WorkMail. El dominio de correo de prueba es *alias* .awsapps.com y se usa como dominio predeterminado si no configuras tu propio dominio. El dominio del correo electrónico de prueba está sujeto a diferentes límites. Para obtener más información, consulte WorkMail Cuotas de Amazon.

Directorio

Un conector AD AWS Simple, AD AWS gestionado o AD Connector creado en AWS Directory Service. Si creas una organización mediante la configuración WorkMail rápida de Amazon, crearemos un WorkMail directorio para ti. No puedes ver un WorkMail directorio en AWS Directory Service.

User

Un usuario creado en AWS Directory Service. El usuario se puede crear con un rol USER o REMOTE_USER. Al crear y habilitar un usuario con el rol USER, este recibe su propio buzón de correo al que puede obtener acceso. Cuando un usuario está deshabilitado, no puede acceder a Amazon WorkMail.

Los usuarios creados y habilitados con el rol REMOTE_USER aparecen en la libreta de direcciones, pero no tienen un buzón en Amazon. WorkMail El REMOTE_USER puede tener el buzón alojado fuera de Amazon, WorkMail pero seguirá figurando como cualquier otro usuario con buzón en la libreta de WorkMail direcciones de Amazon y podrá consultar el calendario de los demás usuarios para encontrar información sobre las plazas libres o las ocupadas.

Grupo

Un grupo utilizado en. AWS Directory Service Un grupo se puede utilizar como lista de distribución o grupo de seguridad en Amazon WorkMail. Los grupos no tienen buzones de correo propios.

Recurso

Un recurso representa una sala de reuniones o un recurso de equipo que WorkMail los usuarios de Amazon pueden reservar.

Política de dispositivos móviles

Diferentes reglas sobre la política de TI que controlan las características de seguridad y el comportamiento de un dispositivo móvil.

Servicios de AWS relacionados

Los siguientes servicios se utilizan junto con Amazon WorkMail:

- AWS Directory Service—Puede integrar Amazon WorkMail con un conector AWS Simple AD, AD AWS gestionado o AD Connector existente. Cree un directorio en AWS Directory Service y, a continuación, active Amazon WorkMail para este directorio. Tras configurar esta integración, puede elegir qué usuarios quiere habilitar para Amazon de una lista WorkMail de usuarios de su directorio actual, y los usuarios pueden iniciar sesión con sus credenciales de Active Directory existentes. Para obtener más información, consulte Guía de administración de AWS Directory Service.
- Amazon Simple Email Service: Amazon WorkMail usa Amazon SES para enviar todos los correos salientes. El dominio de correo de prueba y sus dominios están disponibles para su administración en la consola de Amazon SES. Los correos salientes enviados desde Amazon no tienen coste alguno WorkMail. Para obtener más información, consulte Guía para desarrolladores de Amazon Simple Email Service.
- AWS Identity and Access Management AWS Management Console —Requiere su nombre de usuario y contraseña para que cualquier servicio que utilice pueda determinar si tiene permiso para acceder a sus recursos. Le recomendamos que evite usar las credenciales de las cuentas de AWS para acceder, AWS ya que las credenciales de las AWS cuentas no se pueden revocar ni limitar de ninguna manera. En cambio, le recomendamos que cree un usuario de IAM y añada el usuario a un grupo de IAM con permisos administrativos. A continuación, puede acceder a la consola utilizando las credenciales de usuario de IAM.

  Si se ha inscrito en AWS pero no ha creado un usuario de IAM para usted, puede crearlo en la consola de IAM. Para obtener más información, consulte Creación de usuarios de IAM individuales en la Guía del usuario de IAM.
- AWS Key Management Service—Amazon WorkMail está integrado AWS KMS para cifrar los datos de los clientes. La administración de claves se puede realizar desde la AWS KMS consola. Para obtener más información, consulte ¿Qué es AWS Key Management Service? en la Guía para desarrolladores de AWS Key Management Service .

WorkMail Precios de Amazon

Con Amazon WorkMail, no hay comisiones ni compromisos por adelantado. Solo paga por cuentas de usuario activas. Para obtener información específica sobre los precios, consulte Precios.

WorkMail Recursos de Amazon

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con este servicio.

- Clases y talleres: enlaces a cursos especializados y basados en roles, además de laboratorios autoguiados para mejorar tus AWS habilidades y adquirir experiencia práctica.
- AWS Centro para desarrolladores: explore los tutoriales, descargue herramientas y obtenga información sobre los eventos para desarrolladores. AWS
- AWS Herramientas para desarrolladores: enlaces a herramientas para desarrolladores SDKs, kits de herramientas IDE y herramientas de línea de comandos para desarrollar y administrar AWS aplicaciones.
- Centro de recursos de introducción: aprenda a configurar su aplicación Cuenta de AWS, a unirse a la AWS comunidad y a lanzar su primera aplicación.
- Tutoriales prácticos: sigue step-by-step los tutoriales para lanzar tu primera aplicación. AWS
- AWS Documentos técnicos: enlaces a una lista completa de AWS documentos técnicos, que abarcan temas como la arquitectura, la seguridad y la economía, redactados por arquitectos de AWS soluciones u otros expertos técnicos.
- AWS Support Center: el centro para crear y gestionar sus casos. AWS Support También incluye enlaces a otros recursos útiles, como foros, información técnica FAQs, estado del servicio y AWS Trusted Advisor.
- Soporte— La página web principal con información sobre Soporte un one-on-one canal de soporte de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en la nube.
- Contacta con nosotros – Un punto central de contacto para las consultas relacionadas con la facturación AWS , cuentas, eventos, abuso y demás problemas.
- AWS Condiciones del sitio: información detallada sobre nuestros derechos de autor y marca comercial; su cuenta, licencia y acceso al sitio; y otros temas.

Requisitos previos

Para actuar como WorkMail administrador de Amazon, necesitas una cuenta de AWS. Si aún no se ha inscrito en AWS, complete las siguientes tareas.

Temas

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro implica recibir una llamada telefónica o un mensaje de texto e introducir un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Conceder permisos a los usuarios de IAM para Amazon WorkMail

De forma predeterminada, los usuarios de IAM no tienen permisos para gestionar los WorkMail recursos de Amazon. Debe adjuntar una política administrada por AWS (AmazonWorkMailFullAccesso AmazonWorkMailReadOnlyAccess) o crear una política administrada por el cliente que conceda esos permisos de forma explícita a los usuarios de IAM. A continuación, adjunte la política a los usuarios o grupos de IAM que necesiten esos permisos. Para obtener más información, consulte Gestión de identidades y accesos para Amazon WorkMail.

Seguridad en Amazon WorkMail

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Amazon WorkMail, consulta AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: tu responsabilidad viene determinada por el AWS servicio que utilices. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación te ayuda a entender cómo aplicar el modelo de responsabilidad compartida cuando utilizas Amazon WorkMail. En los temas siguientes, se muestra cómo configurar Amazon WorkMail para que cumpla con sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros servicios de AWS que le ayudan a supervisar y proteger sus WorkMail recursos de Amazon.

Temas

Protección de datos en Amazon WorkMail

El AWS modelo de se aplica a protección de datos en Amazon WorkMail. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Amazon WorkMail u otra Servicios de AWS empresa mediante la consola, la API o AWS SDKs. AWS CLI Cualquier dato que ingrese en

etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cómo WorkMail usa Amazon AWS KMS

Amazon cifra de WorkMail forma transparente todos los mensajes de los buzones de todas WorkMail las organizaciones de Amazon antes de que los mensajes se escriban en el disco y los descifra de forma transparente cuando los usuarios acceden a ellos. No puede deshabilitar el cifrado. Para proteger las claves de cifrado que protegen los mensajes, Amazon WorkMail está integrado con AWS Key Management Service (AWS KMS).

Amazon WorkMail también ofrece una opción para permitir a los usuarios enviar correos electrónicos firmados o cifrados. Esta característica de cifrado no utiliza AWS KMS. Para obtener más información, consulte Habilitación del correo electrónico firmado o cifrado.

Temas

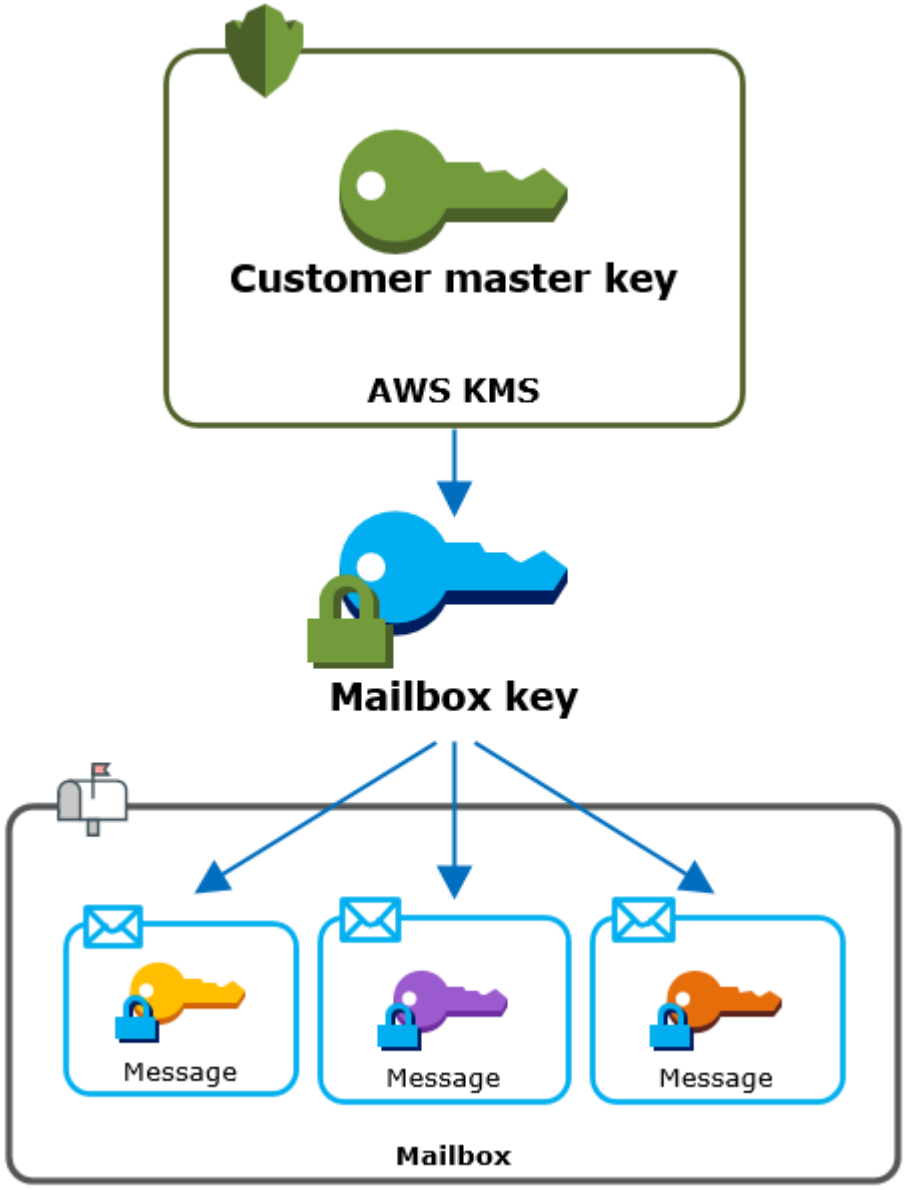
WorkMail Cifrado de Amazon

En Amazon WorkMail, cada organización puede contener varios buzones, uno para cada usuario de la organización. Todos los mensajes, incluido los elementos de correo electrónico y de calendario, se almacenan en el buzón de correo del usuario.

Para proteger el contenido de los buzones de sus WorkMail organizaciones de Amazon, Amazon WorkMail cifra todos los mensajes de los buzones antes de escribirlos en el disco. Ninguno de los datos proporcionados por el cliente se almacena en texto no cifrado.

Cada mensaje se cifra con una clave de cifrado de datos única. La clave del mensaje se protege con una clave del buzón de correo, que es una clave de cifrado única que se utiliza únicamente para ese buzón de correo. La clave del buzón se cifra con una clave maestra AWS KMS del cliente (CMK) para la organización, que nunca se queda sin cifrar. AWS KMS En el siguiente diagrama se muestra

la relación de los mensajes cifrados, claves de mensaje cifradas, clave de buzón de correo cifrada y la CMK de la organización en AWS KMS.



Establecimiento de una CMK para la organización

Al crear una WorkMail organización de Amazon, tienes la opción de seleccionar una clave maestra de AWS KMS cliente (CMK) para la organización. Esta CMK protege todas las claves de buzón de correo de esa organización.

Puedes seleccionar la CMK AWS gestionada por defecto para Amazon WorkMail o puedes seleccionar una CMK gestionada por un cliente existente que te pertenezca y gestione. Para obtener más información, consulta las claves maestras del cliente (CMKs) en la Guía AWS Key Management

Service para desarrolladores. Puede seleccionar la misma CMK o una CMK diferente para cada una de sus organizaciones, pero no puede cambiar la CMK una vez que la haya seleccionado.

> **Important**
>
> Amazon solo WorkMail admite sistemas simétricos CMKs. No puede utilizar una CMK asimétrica. Para obtener ayuda para determinar si una CMK es simétrica o asimétrica, consulte Identificación de simétricas y CMKs asimétricas en la Guía para desarrolladores.AWS Key Management Service

Para encontrar la CMK de su organización, utilice la entrada de AWS CloudTrail registro que registra las llamadas a. AWS KMS

Clave de cifrado única para cada buzón de correo

Al crear un buzón, Amazon WorkMail genera una clave de cifrado simétrica AES (Advanced Encryption Standard) exclusiva de 256 bits para el buzón, conocida como clave de buzón, fuera de. AWS KMS Amazon WorkMail usa la clave del buzón para proteger las claves de cifrado de cada mensaje del buzón.

Para proteger la clave del buzón, Amazon WorkMail pide AWS KMS que se cifre la clave del buzón en la CMK de la organización. A continuación, almacena la clave del buzón de correo cifrada en los metadatos del buzón.

> **Note**
>
> Amazon WorkMail utiliza una clave de cifrado de buzones simétrica para proteger las claves de los mensajes. Anteriormente, Amazon WorkMail protegía cada buzón con un key pair asimétrico. Utilizaba la clave pública para cifrar cada clave del mensaje y la clave privada para descifrarla. La clave privada del buzón de correo se protegía con la CMK de la organización. Los buzones de correo más antiguos podrían utilizar un par de claves de buzón de correo asimétricas. Este cambio no afecta a la seguridad de la bandeja de entrada ni de sus mensajes.

Cifrado de cada mensaje

Cuando un usuario añade un mensaje a un buzón, Amazon WorkMail genera una clave de cifrado simétrica AES única de 256 bits para el mensaje externo a. AWS KMS Utiliza esta clave de mensaje

para cifrar el mensaje. Amazon WorkMail cifra la clave del mensaje debajo de la clave del buzón y guarda la clave del mensaje cifrado junto con el mensaje. A continuación, cifra la clave de buzón de correo con la CMK de la organización.

Creación de un nuevo buzón de correo

Cuando Amazon WorkMail crea un buzón de correo, utiliza el siguiente proceso para prepararlo para contener los mensajes cifrados.

- Amazon WorkMail genera una clave de cifrado simétrica AES única de 256 bits para el buzón fuera de AWS KMS.
- Amazon WorkMail llama a la operación AWS KMS Encrypt. Transmite la clave del buzón y el identificador de la clave maestra del cliente (CMK) de la organización. AWS KMS devuelve un texto cifrado de la clave del buzón cifrada en la CMK.
- Amazon WorkMail almacena la clave del buzón cifrada con los metadatos del buzón.

Cifrar un mensaje del buzón de correo

Para cifrar un mensaje, Amazon WorkMail utiliza el siguiente proceso.

1. Amazon WorkMail genera una clave simétrica AES única de 256 bits para el mensaje. Utiliza la clave del mensaje de texto sin formato y el algoritmo del Estándar de Encriptación Avanzada (AES) para cifrar el mensaje desde fuera de. AWS KMS
2. Para proteger la clave del mensaje que se encuentra debajo de la clave del buzón, Amazon WorkMail necesita descifrar la clave del buzón, que siempre se almacena cifrada.

   Amazon WorkMail llama a la operación de AWS KMS descifrado y pasa la clave del buzón cifrada. AWS KMS usa la CMK para que la organización descifre la clave del buzón y devuelve la clave de buzón de texto sin formato a Amazon. WorkMail
3. Amazon WorkMail utiliza la clave de buzón de texto sin formato y el algoritmo del Estándar de cifrado avanzado (AES) para cifrar la clave del mensaje fuera de. AWS KMS
4. Amazon WorkMail almacena la clave del mensaje cifrado en los metadatos del mensaje cifrado para que esté disponible para descifrarlo.

Descifrar un mensaje del buzón de correo

Para descifrar un mensaje, Amazon WorkMail utiliza el siguiente proceso.

1. Amazon WorkMail llama a la operación de AWS KMS descifrado y pasa la clave del buzón cifrada. AWS KMS usa la CMK para que la organización descifre la clave del buzón y devuelve la clave de buzón de texto sin formato a Amazon. WorkMail
2. Amazon WorkMail utiliza la clave de buzón de texto sin formato y el algoritmo del Estándar de cifrado avanzado (AES) para descifrar la clave del mensaje cifrado fuera de. AWS KMS
3. Amazon WorkMail utiliza la clave del mensaje de texto sin formato para descifrar el mensaje cifrado.

Almacenamiento en caché de las claves del buzón de correo

Para mejorar el rendimiento y minimizar las llamadas a AWS KMS, Amazon almacena en WorkMail caché cada clave de buzón de texto simple de cada cliente de forma local durante un máximo de un minuto. Al final del período de almacenamiento en caché, la clave del buzón de correo se elimina. Si se requiere la clave del buzón de ese cliente durante el período de almacenamiento en caché, Amazon WorkMail puede obtenerla de la memoria caché en lugar de llamar AWS KMS. La clave del buzón de correo está protegida en la memoria caché y nunca se escribe en disco en texto sin formato.

Autorizar el uso de la CMK

Cuando Amazon WorkMail utiliza una clave maestra del cliente (CMK) en las operaciones criptográficas, actúa en nombre del administrador del buzón.

Para utilizar la clave maestra del AWS KMS cliente (CMK) como secreto en su nombre, el administrador debe tener los siguientes permisos. Puede especificar estos permisos necesarios en una política de IAM o política de claves.

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

Para permitir que la CMK se use solo para las solicitudes que se originan en Amazon WorkMail, puedes usar la clave de ViaService condición kms: con el `workmail.<region>.amazonaws.com` valor.

También puede utilizar las claves o los valores en el contexto de cifrado como condición para utilizar la CMK para operaciones criptográficas. Por ejemplo, puede utilizar un operador de condición

de cadena en un IAM o en un documento de política de claves, o bien utilizar una restricción de concesión en una concesión.

Política de claves para la CMK administrada de AWS

La política clave de la CMK AWS gestionada para Amazon WorkMail otorga a los usuarios permiso para utilizar la CMK para operaciones específicas solo cuando Amazon WorkMail realiza la solicitud en nombre del usuario. La política de claves no permite a ningún usuario utilizar la CMK directamente.

Esta política de claves, como las políticas de todas las claves administradas por AWS, la establece el servicio. No puede cambiar la política de claves, pero puede verla en cualquier momento. Para obtener más información, consulte Visualización de una política de claves en la Guía para desarrolladores de AWS Key Management Service .

Las declaraciones de política de la política de claves tienen el siguiente efecto:

- Permita que los usuarios de la cuenta y la región utilicen la CMK para operaciones criptográficas y para crear subvenciones, pero solo cuando la solicitud provenga de Amazon WorkMail en su nombre. La clave de condición `kms:ViaService` aplica esta restricción.
- Permite a la AWS cuenta crear políticas de IAM que permitan a los usuarios ver las propiedades de la CMK y revocar las subvenciones.

La siguiente es una política clave para un ejemplo de CMK AWS gestionado para 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" : "*"
  } ]
}
```

Uso de subvenciones para autorizar a Amazon WorkMail

Además de las políticas clave, Amazon WorkMail utiliza las subvenciones para añadir permisos a la CMK para cada organización. Para ver las concesiones en la CMK de su cuenta, utilice la ListGrantsoperación.

Amazon WorkMail utiliza las concesiones para añadir los siguientes permisos a la CMK de la organización.

- Añade el `kms:Encrypt` permiso para permitir que Amazon WorkMail cifre la clave del buzón.
- Añada el `kms:Decrypt` permiso para permitir que Amazon WorkMail utilice la CMK para descifrar la clave del buzón. Amazon WorkMail requiere este permiso en una concesión porque la solicitud de lectura de los mensajes del buzón utiliza el contexto de seguridad del usuario que lee el mensaje. La solicitud no utiliza las credenciales de la AWS cuenta. Amazon WorkMail crea esta subvención cuando seleccionas una CMK para la organización.

Para crear las subvenciones, Amazon WorkMail llama CreateGranten nombre del usuario que creó la organización. El permiso para crear la concesión proviene de la política de claves. Esta política permite a los usuarios de cuentas `CreateGrant` recurrir a la CMK de la organización cuando Amazon WorkMail realiza la solicitud en nombre de un usuario autorizado.

La política de claves también permite al administrador de la cuenta revocar la concesión de la clave AWS gestionada. Sin embargo, si revocas la concesión, Amazon no WorkMail podrá descifrar los datos cifrados de tus buzones.

Contexto WorkMail de cifrado de Amazon

Un contexto de cifrado es un conjunto de pares de clave-valor que contienen datos no secretos arbitrarios. Cuando incluye un contexto de cifrado en una solicitud de cifrado de datos, vincula AWS KMS criptográficamente el contexto de cifrado a los datos cifrados. Para descifrar los datos, es necesario pasar el mismo contexto de cifrado. Para obtener más información, consulte Contexto de cifrado en la Guía para desarrolladores de AWS Key Management Service .

Amazon WorkMail utiliza el mismo formato de contexto de cifrado en todas las operaciones AWS KMS criptográficas. Puede utilizar el contexto de cifrado para identificar una operación criptográfica en los registros y registros de auditoría, como AWS CloudTrail y como una condición para la autorización en las políticas y concesiones.

En sus solicitudes de cifrado y descifrado, AWS KMS Amazon WorkMail utiliza un contexto de cifrado en el que la clave está `aws:workmail:arn` y el valor es el nombre de recurso de Amazon (ARN) de la organización.

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

Por ejemplo, el siguiente contexto de cifrado incluye un ARN de organización de ejemplo en la región de Europa (Irlanda) (`eu-west-1`).

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

Supervisión de la WorkMail interacción de Amazon con AWS KMS

Puedes usar AWS CloudTrail Amazon CloudWatch Logs para realizar un seguimiento de las solicitudes que Amazon WorkMail envía AWS KMS en tu nombre.

Encrypt

Al crear un buzón, Amazon WorkMail genera una clave de buzón y llama AWS KMS para cifrarla. Amazon WorkMail envía una solicitud de cifrado a AWS KMS con la clave del buzón de correo en texto simple y un identificador para la CMK de la organización de Amazon. WorkMail

El evento que registra la operación `Encrypt` es similar al siguiente evento de ejemplo. El usuario es el WorkMail servicio de Amazon. Los parámetros incluyen el ID de CMK (`keyId`) y el contexto de cifrado de la WorkMail organización de Amazon. Amazon WorkMail también pasa la clave del buzón, pero no queda registrada en el 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

Cuando añades, ves o eliminas un mensaje del buzón, Amazon WorkMail te pide AWS KMS que descifre la clave del buzón. Amazon WorkMail envía una solicitud de descifrado a AWS KMS con la clave del buzón cifrada y un identificador para la CMK de la organización de Amazon WorkMail.

El evento que registra la operación `Decrypt` es similar al siguiente evento de ejemplo. El usuario es el WorkMail servicio de Amazon. Los parámetros incluyen la clave del buzón de correo cifrada (como un blob de texto cifrado), que no se registra en el registro, y el contexto de cifrado de la organización de Amazon. WorkMail AWS KMS obtiene el identificador de la CMK a partir del texto cifrado.


```
{
    "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"
}
```

Gestión de identidades y accesos para Amazon WorkMail

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Amazon WorkMail . El IAM es un Servicio de AWS servicio que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Amazon WorkMail.

Usuario del servicio: si utilizas el WorkMail servicio de Amazon para realizar tu trabajo, el administrador te proporcionará las credenciales y los permisos que necesitas. A medida que utilices más WorkMail funciones de Amazon para realizar tu trabajo, es posible que necesites permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puedes acceder a una función de Amazon WorkMail, consultaSolución de problemas de WorkMail identidad y acceso a Amazon.

Administrador de servicios: si estás a cargo de WorkMail los recursos de Amazon en tu empresa, probablemente tengas acceso total a Amazon WorkMail. Es tu trabajo determinar a qué WorkMail funciones y recursos de Amazon deben acceder los usuarios de tu servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Amazon WorkMail, consulteCómo WorkMail funciona Amazon con IAM.

Administrador de IAM: si eres administrador de IAM, quizá te interese obtener más información sobre cómo puedes redactar políticas para gestionar el acceso a Amazon. WorkMail Para ver ejemplos de políticas WorkMail basadas en la identidad de Amazon que puedes usar en IAM, consulta. Ejemplos de políticas WorkMail basadas en la identidad de Amazon

Autenticación con identidades

La autenticación es la forma en que inicias sesión para AWS usar tus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el

usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulta Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puedes crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad

al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .

- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puedes utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades puedes clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas puedes establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo WorkMail funciona Amazon con IAM

Antes de utilizar IAM para gestionar el acceso a Amazon WorkMail, debes entender qué funciones de IAM están disponibles para su uso con Amazon. WorkMail Para obtener una visión general de cómo Amazon WorkMail y otros AWS servicios funcionan con IAM, consulta AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Temas

- Políticas de Amazon WorkMail basadas en la identidad
- Políticas de Amazon WorkMail basadas en recursos
- Autorización basada en WorkMail etiquetas de Amazon
- Funciones de Amazon WorkMail IAM

Políticas de Amazon WorkMail basadas en la identidad

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Amazon WorkMail admite acciones, recursos y claves de condición específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas en Amazon WorkMail utilizan el siguiente prefijo antes de la acción:`workmail:`. Por ejemplo, para conceder permiso a alguien para recuperar una lista de usuarios con la operación de la WorkMail `ListUsers` API de Amazon, debes incluir la `workmail:ListUsers` acción en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Amazon WorkMail define su propio conjunto de acciones que describen las tareas que puedes realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

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

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción:

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

Para ver una lista de WorkMail las acciones de Amazon, consulta Acciones definidas por Amazon WorkMail en la Guía del usuario de IAM.

Recursos

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Amazon WorkMail admite permisos a nivel de recursos para las organizaciones de Amazon WorkMail .

El recurso de WorkMail la organización Amazon tiene el siguiente ARN:

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

Para obtener más información sobre el formato de ARNs, consulte Nombres de recursos de Amazon (ARNs) y espacios de nombres AWS de servicios.

Por ejemplo, para especificar la organización `m-n1pq2345678r901st2u3vx45x6789yza` en la instrucción, utilice el siguiente ARN.

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

Para especificar todas las organizaciones que pertenecen a una cuenta específica, utilice el carácter comodín (*):

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

Algunas WorkMail acciones de Amazon, como las de creación de recursos, no se pueden realizar en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

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

Para ver una lista de los tipos de WorkMail recursos de Amazon y sus tipos ARNs, consulta Recursos definidos por Amazon WorkMail en la Guía del usuario de IAM. Para obtener información sobre las acciones que puede especificar para el ARN de cada recurso, consulte Acciones, recursos y claves de condición de Amazon. WorkMail

Claves de condición

Amazon WorkMail admite las siguientes claves de condición globales.

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

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

El siguiente ejemplo de política concede acceso a la WorkMail consola de Amazon únicamente a los directores de IAM autenticados por MFA en la región de AWS. eu-west-1

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

Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

`workmail:ImpersonationRoleIdes` la única clave de condición específica del servicio que admite Amazon. WorkMail

El siguiente ejemplo de política limita la `AssumeImpersonationRole` acción a una organización y a una función de suplantación de identidad en particular WorkMail .

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

Ejemplos

Para ver ejemplos de políticas de Amazon WorkMail basadas en la identidad, consulta. Ejemplos de políticas WorkMail basadas en la identidad de Amazon

Políticas de Amazon WorkMail basadas en recursos

Amazon WorkMail no admite políticas basadas en recursos.

Autorización basada en WorkMail etiquetas de Amazon

Puedes adjuntar etiquetas a WorkMail los recursos de Amazon o pasarlas en una solicitud a Amazon WorkMail. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición

`aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Para obtener más información sobre el etiquetado de WorkMail los recursos de Amazon, consulteEtiquetado de una organización.

Funciones de Amazon WorkMail IAM

Un rol de IAM es una entidad de su AWS cuenta que tiene permisos específicos.

Uso de credenciales temporales con Amazon WorkMail

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de AWS STS API como AssumeRoleo GetFederationToken.

Amazon WorkMail admite el uso de credenciales temporales.

Roles vinculados a servicios

Los roles vinculados a un servicio permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en tu nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Amazon WorkMail admite funciones vinculadas a servicios. Para obtener más información sobre la creación o la gestión de funciones WorkMail vinculadas a los servicios de Amazon, consulte. Uso de roles vinculados a servicios para Amazon WorkMail

Roles de servicio

Esta característica permite que un servicio asuma un rol de servicio en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Amazon WorkMail apoya las funciones de servicio.

Ejemplos de políticas WorkMail basadas en la identidad de Amazon

De forma predeterminada, los usuarios y roles de IAM no tienen permiso para crear o modificar WorkMail los recursos de Amazon. Tampoco pueden realizar tareas mediante la AWS API AWS Management Console AWS CLI, o. Un administrador de IAM debe crear políticas de IAM que

concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas
- Uso de la WorkMail consola de Amazon
- Permitir a los usuarios consultar sus propios permisos
- Permitir a los usuarios el acceso de solo lectura a los recursos de Amazon WorkMail

Prácticas recomendadas relativas a políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar WorkMail los recursos de Amazon de tu cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse

utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la WorkMail consola de Amazon

Para acceder a la WorkMail consola de Amazon, debes tener un conjunto mínimo de permisos. Estos permisos deben permitirte enumerar y ver detalles sobre los WorkMail recursos de Amazon de tu AWS cuenta. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

Para garantizar que esas entidades puedan seguir utilizando la WorkMail consola de Amazon, adjunta también la siguiente política AWS gestionada, AmazonWorkMailFullAccess, a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

La AmazonWorkMailFullAccesspolítica otorga a los usuarios de IAM acceso total a WorkMail los recursos de Amazon. Esta política otorga al usuario acceso a todas las AWS Directory Service operaciones y servicios de Amazon WorkMail AWS Key Management Service, Amazon Simple Email Service. Esto también incluye varias EC2 operaciones de Amazon que Amazon WorkMail necesita realizar en tu nombre. Los `cloudwatch` permisos `logs` y son necesarios para registrar eventos

de correo electrónico y ver las métricas en la WorkMail consola de Amazon. El registro de auditoría utiliza CloudWatch Logs, Amazon S3 y Amazon Data FireHose para almacenar`logs`. Para obtener más información, consulte Registro y supervisión en 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"
```

```
            }
        }
    }
  ]
}
```

No es necesario conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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": "*"
        }
    ]
}
```

Permitir a los usuarios el acceso de solo lectura a los recursos de Amazon WorkMail

La siguiente declaración de política concede a los usuarios de IAM acceso de solo lectura a los recursos de Amazon. WorkMail Esta política proporciona el mismo nivel de acceso que la política gestionada por AWS AmazonWorkMailReadOnlyAccess. Cualquiera de las dos políticas permite al usuario acceder a todas las WorkMail `Describe` operaciones de Amazon. El acceso a la AWS Directory Service `DescribeDirectories` operación es necesario para obtener información sobre sus AWS Directory Service directorios. El acceso al servicio Amazon SES es necesario para obtener información sobre los dominios configurados. El acceso a AWS Key Management Service es necesario para obtener información sobre las claves de cifrado utilizadas. Los `cloudwatch` permisos `logs` y son necesarios para registrar eventos de correo electrónico y ver las métricas en la WorkMail consola de Amazon. El registro de auditoría utiliza CloudWatch Logs, Amazon S3 y Amazon Data FireHose para almacenar`logs`. Para obtener más información, consulte Registro y supervisión en 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": "*"
    }
  ]
}
```

Solución de problemas de WorkMail identidad y acceso a Amazon

Utiliza la siguiente información para ayudarte a diagnosticar y solucionar los problemas habituales que puedes encontrar al trabajar con Amazon WorkMail e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en Amazon WorkMail
- No estoy autorizado a realizar lo siguiente: PassRole
- Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis WorkMail recursos de Amazon

No estoy autorizado a realizar ninguna acción en Amazon WorkMail

Si AWS Management Console te indica que no estás autorizado a realizar una acción, debes ponerte en contacto con tu administrador para obtener ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

El siguiente ejemplo de error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para ver detalles de un grupo pero no tiene permisos `workmail:DescribeGroup`.

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

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso `group` mediante la acción `workmail:DescribeGroup`.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibes un error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a Amazon WorkMail.

Algunas te Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon WorkMail. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesitas ayuda, ponte en contacto con tu AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis WorkMail recursos de Amazon

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon WorkMail admite estas funciones, consultaCómo WorkMail funciona Amazon con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

AWS políticas gestionadas para Amazon WorkMail

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política gestionada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AmazonWorkMailFullAccess

Puede adjuntar la política `AmazonWorkMailFullAccess` a las identidades de IAM. Esta política otorga permisos que permiten el acceso total a Amazon WorkMail.

Para ver los permisos de esta política, consulte AmazonWorkMailFullAccess en la AWS Management Console.

AWS política gestionada: AmazonWorkMailReadOnlyAccess

Puede adjuntar la política `AmazonWorkMailReadOnlyAccess` a las identidades de IAM. Esta política concede permisos que permiten el acceso de solo lectura a Amazon. WorkMail

Para ver los permisos de esta política, consulte AmazonWorkMailReadOnlyAccess en la AWS Management Console.

AWS política gestionada: AmazonWorkMailEventsServiceRolePolicy

Esta política se adjunta a la función vinculada al servicio denominada AmazonWorkMailEventspara permitir el acceso a AWS los servicios y recursos utilizados o gestionados por Amazon WorkMail Events. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon WorkMail.

Amazon WorkMail actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon WorkMail desde que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
Actualizaciones de políticas administradas por AWS: actualización de una política existente	Se actualizaron `AmazonWorkMailFullAccess` los permisos `AmazonWorkMailReadOnlyAccess` y para WorkMail que Amazon admita el registro de auditorías. Para obtener más información sobre los	14 de febrero de 2024

Cambio	Descripción	Fecha
	permisos actualizados, consulte Ejemplos de políticas WorkMail basadas en la identidad de Amazon y para obtener información sobre el registro de auditorías, consulteHabilitación del registro de auditoría.	
Amazon WorkMail comenzó a rastrear los cambios	Amazon WorkMail comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	1 de marzo de 2021

Uso de roles vinculados a servicios para Amazon WorkMail

Amazon WorkMail usa roles AWS Identity and Access Management vinculados a servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon. WorkMail Amazon predefine las funciones vinculadas al servicio WorkMail e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre.

Un rol vinculado a un servicio facilita la configuración de Amazon WorkMail porque no tienes que añadir manualmente los permisos necesarios. Amazon WorkMail define los permisos de sus funciones vinculadas a servicios y, a menos que se defina lo contrario, solo Amazon WorkMail puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar los recursos relacionados. Esto protege tus WorkMail recursos de Amazon porque no puedes eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que tienen Sí en la columna Rol vinculado a servicio. Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Amazon WorkMail

Amazon WorkMail usa el rol vinculado al servicio denominado — AmazonWorkMailEventsAmazon WorkMail usa este rol vinculado al servicio para permitir el acceso a los AWS servicios y recursos utilizados o gestionados por los eventos de Amazon, como la supervisión de WorkMail los eventos de correo electrónico registrados por. CloudWatch Para obtener más información sobre cómo habilitar el registro de eventos de correo electrónico para Amazon WorkMail, consulteHabilitar el registro de eventos por correo electrónico.

El rol AmazonWorkMailEvents vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `events.workmail.amazonaws.com`

La política de permisos de roles permite WorkMail a Amazon realizar las siguientes acciones en los recursos especificados:

- Acción: `logs:CreateLogGroup` en `all AWS resources`
- Acción: `logs:CreateLogStream` en `all AWS resources`
- Acción: `logs:PutLogEvents` en `all AWS resources`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear un rol vinculado a un servicio para Amazon WorkMail

No necesita crear manualmente un rol vinculado a servicios. Cuando activas el registro de WorkMail eventos de Amazon y utilizas la configuración predeterminada de la WorkMail consola de Amazon, Amazon WorkMail crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando activas el registro de WorkMail eventos de Amazon y utilizas la configuración predeterminada, Amazon vuelve a WorkMail crear el rol vinculado al servicio para ti.

Edición de un rol vinculado a un servicio para Amazon WorkMail

Amazon WorkMail no te permite editar el rol AmazonWorkMailEvents vinculado al servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Edición de un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para Amazon WorkMail

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el WorkMail servicio de Amazon utiliza el rol cuando intentas eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar WorkMail los recursos de Amazon utilizados por AmazonWorkMailEvents

1. Desactiva el registro de WorkMail eventos de Amazon.

    a. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

    Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

    b. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.

    c. En el panel de navegación, elija Configuración de la organización y, a continuación, Monitoreo.

    d. Para la configuración de registro, elija Edit (Editar).

    e. Mueva el control deslizante Habilitar eventos de correo a la posición desactivado.

f. Seleccione Guardar.

2. Elimina el grupo de CloudWatch registros de Amazon.

   a. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.

   b. Seleccione Logs (Registros).

   c. En Log Groups (Grupo de registros), seleccione el grupo de registros que desea eliminar.

   d. En Actions (Acciones), seleccione Delete log group (Eliminar grupo de registros) .

   e. Elija Yes, Delete (Sí, eliminar).

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AmazonWorkMailEvents servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para los roles vinculados a WorkMail los servicios de Amazon

Amazon WorkMail admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte Amazon WorkMail Regions and Endpoints.

Registro y supervisión en Amazon WorkMail

Supervisar y auditar tu correo electrónico y tus registros es importante para mantener la salud de tu WorkMail organización de Amazon. Amazon WorkMail admite dos tipos de monitorización:

- Registro de eventos: monitorear la actividad de envío de correos electrónicos de su organización ayuda a proteger la reputación de su dominio. La monitorización también puede ayudarle a realizar un seguimiento de correos electrónicos que se envían y reciben. Para obtener más información acerca de cómo habilitar el registro de eventos de correo electrónico, consulte Habilitar el registro de eventos por correo electrónico.
- Registro de auditoría: puedes usar los registros de auditoría para recopilar información detallada sobre el uso de tu WorkMail organización de Amazon, como monitorear el acceso de los usuarios a los buzones, auditar para detectar actividades sospechosas y depurar las configuraciones de

los proveedores de disponibilidad y control de acceso. Para obtener más información, consulte Habilitación del registro de auditoría.

AWS proporciona las siguientes herramientas de supervisión para vigilar Amazon WorkMail, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Por ejemplo, si habilitas el registro de eventos por correo electrónico para Amazon WorkMail, CloudWatch podrás realizar un seguimiento de los correos electrónicos enviados y recibidos de tu organización. Para obtener más información sobre cómo monitorizar Amazon WorkMail con CloudWatch, consultaMonitorización de Amazon WorkMail con CloudWatch métricas. Para obtener más información al respecto CloudWatch, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus eventos de correo electrónico y registros de auditoría para Amazon WorkMail cuando el registro de correo electrónico y auditoría está activado en la WorkMail consola de Amazon. CloudWatch Los registros pueden monitorear la información de los archivos de registro y puedes archivar los datos de registro en un almacenamiento de alta durabilidad. Para obtener más información sobre el seguimiento de WorkMail los mensajes de Amazon mediante CloudWatch Logs, consulta Habilitar el registro de eventos por correo electrónico yHabilitación del registro de auditoría. Para obtener más información sobre CloudWatch los registros, consulta la Guía del usuario de Amazon CloudWatch Logs.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por usted o en su Cuenta de AWS nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para obtener más información, consulte Registrar llamadas a WorkMail la API de Amazon con AWS CloudTrail.
- Amazon S3 le permite almacenar sus WorkMail eventos de Amazon y acceder a ellos de forma rentable. Amazon S3 proporciona mecanismos para administrar el ciclo de vida de los datos de los eventos, lo que le permite configurar la eliminación automática de eventos antiguos o configurar el archivado automático en Amazon S3 Glacier. Tenga en cuenta que Amazon S3 solo está disponible para eventos de registro de auditoría. Para obtener más información sobre Amazon S3, consulte la Guía del usuario de Amazon S3.
- Amazon Data Firehose le permite transmitir los datos de sus eventos a otros servicios de AWS, como Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Service, OpenSearch Amazon Serverless, Splunk y cualquier punto de enlace HTTP o punto de enlace

HTTP personalizado propiedad de proveedores de servicios externos compatibles, incluidos Datadog, LogicMonitor Dynatrace, MongoDB, New Relic, Coralogix y Elastic. OpenSearch La entrega a Firehose solo está disponible para eventos de registro de auditoría. Para obtener más información sobre Firehose, consulte la guía para desarrolladores de Amazon Data Firehose.

Temas

Monitorización de Amazon WorkMail con CloudWatch métricas

Puedes monitorizar el WorkMail uso de Amazon CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Las métricas gratuitas se almacenan durante 15 meses para que puedas acceder a la información histórica y ver el rendimiento de tu aplicación o servicio web. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

CloudWatch métricas de Amazon WorkMail

Amazon WorkMail envía la siguiente información de métricas y dimensiones a CloudWatch.

El espacio de nombres de `AWS/WorkMail` incluye las siguientes métricas.

Métrica	Descripción
`OrganizationEmailReceived`	El número de correos electrónicos recibidos por tu WorkMail organización de Amazon. Si un correo electrónico está dirigido a 10 destinatarios de tu organización, el `OrganizationEmailReceived` recuento es uno.

Métrica	Descripción
	Unidades: recuento
`MailboxEmailDelivered`	El número de correos electrónicos enviados a los buzones individuales de tu WorkMail organización de Amazon. Si un correo electrónico se entrega correctamente a 10 destinatarios de su organización, el `MailboxEmailDelivered` recuento es de 10. Unidades: recuento
`IncomingEmailBounced`	El número de correos electrónicos entrantes que rebotaron debido a buzones de correo llenos. Esta métrica se cuenta para cada destinatario. Por ejemplo, si se envía un correo electrónico a 10 destinatarios de su organización y dos de los destinatarios tienen buzones llenos, lo que provoca una respuesta de rebote, el `IncomingEmailBounced` recuento es de dos. Unidades: recuento
`OutgoingEmailBounced`	El número de correos salientes que no se han podido entregar. Esta métrica se cuenta para cada destinatario. Por ejemplo, si se envía un correo electrónico a 10 destinatarios y no se han podido entregar dos, el `OutgoingEmailBounced` recuento es 2. Unidades: recuento

Métrica	Descripción
`OutgoingEmailSent`	El número de correos electrónicos enviados correctamente desde tu WorkMail organizac ión de Amazon. Esta métrica se cuenta para cada destinatario de un correo electrónico enviado correctamente. Por ejemplo, si se envía 1 correo electrónico a 10 destinatarios, y el correo electrónico se ha enviado correctam ente a 8 de los destinatarios, el `OutgoingE mailSent` recuento es 8. Unidades: recuento
`AuthenticationFailure`	Esta métrica cuenta el número de intentos de autenticación. Cuando la autenticación se realiza correctamente, el recuento es 0 y cuando la autenticación no se realiza correctam ente, el recuento es 1. Utilice la `Sum` estadísti ca para supervisar la cantidad de intentos de autenticación fallidos. Utilice la `Sample count` estadística para supervisar el número total de eventos de autenticación. Utilice la `Average` estadística para supervisar la proporción de eventos de autenticación fallidos y satisfact orios. Unidades: recuento

Métrica	Descripción
`AccessDenied`	Esta métrica cuenta el número de evaluaciones de control de acceso. Cuando el control de acceso deniega la acción, el recuento es 1 y cuando se concede la acción, el recuento es 0. Utilice la `Sum` estadística para supervisar el volumen de acciones denegadas, la `Sample count` estadística para supervisar el número total de intentos de acción y la `Average` estadística para supervisar la proporción de acciones permitidas y denegadas. Unidades: recuento
`ActionDenied`	Esta métrica se cuenta cuando se toman medidas en los datos del buzón. Cuando se deniega una acción, el recuento es 1 y si se concede la acción, el recuento es 0. Utilice la `Sum` estadística para supervisar el volumen de acciones denegadas en los buzones de correo, la `Sample count` estadística para supervisar el número total de intentos de acciones en el buzón y la `Average` estadística para supervisar la proporción de acciones permitidas y denegadas. Unidades: recuento
`AvailabilityProviderFailure`	Esta métrica se cuenta para cada solicitud del proveedor de disponibilidad que Amazon WorkMail ejecuta para recuperar la disponibilidad del calendario de una fuente externa. Para obtener más información sobre los proveedores de disponibilidad, consulta la Guía del WorkMail administrador de Amazon.

Supervisión de los registros de eventos de WorkMail correo electrónico de Amazon

Cuando activas el registro de eventos por correo electrónico en tu WorkMail organización de Amazon, Amazon WorkMail registra los eventos de correo electrónico con CloudWatch. Para obtener más información acerca de cómo activar el registro de eventos de correo electrónico, consulte Habilitar el registro de eventos por correo electrónico.

En las siguientes tablas se describen los eventos con WorkMail los que Amazon registra CloudWatch, cuándo se transmiten y qué contienen los campos de eventos.

`ORGANIZATION_EMAIL_RECEIVED`

Este evento se registra cuando tu WorkMail organización de Amazon recibe un mensaje de correo electrónico.

Campo	Descripción
recipients	Los destinatarios del mensaje.
remitente	La dirección de correo electrónico del usuario que envió el mensaje de correo electrónico en nombre de otro usuario. Este campo se establece únicamente cuando un mensaje de correo electrónico se envía en nombre de otro usuario.
desde	La dirección From (De), que suele ser la dirección de correo electrónico del usuario que envió el mensaje. Si el usuario envió el mensaje como otro usuario o en nombre de otro usuario, el campo devuelve la dirección de correo electrónico del usuario en cuyo nombre se ha enviado el correo electrónico, no la dirección de correo electrónico del remitente real.
subject	El mensaje de correo electrónico.

Campo	Descripción
messageId	El ID de mensaje de SMTP
spamVerdict	Indica si el mensaje está marcado como spam por Amazon SES. Para obtener más información, consulte Contenido de las notificaciones de recepción de correo electrónico de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.
dkimVerdict	Indica si se ha superado la comprobación del correo DomainKeys identificado (DKIM). Para obtener más información, consulte Contenido de las notificaciones de recepción de correo electrónico de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.
dmarcVerdict	Indica si se ha superado la comprobación de autenticación, notificación y conformidad de los mensajes basada en el dominio (DMARC). Para obtener más información, consulte Contenido de las notificaciones de recepción de correo electrónico de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.
dmarcPolicy	Aparece solo cuando el campo dmarcVerdict contiene «FAIL». Indica la acción que se debe realizar en el correo electrónico cuando se produce un error en la comprobación DMARC (NONE, QUARANTINE, or REJECT). Esto lo establece el propietario del dominio de correo electrónico de envío.

Campo	Descripción
spfVerdict	Indica si se han superado las comprobaciones del Marco de políticas de remitentes (SPF). Para obtener más información, consulte Contenido de las notificaciones de recepción de correo electrónico de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.
messageTimestamp	Indica cuándo se recibe el mensaje.

`MAILBOX_EMAIL_DELIVERED`

Este evento se registra cuando un mensaje se envía a un buzón de correo de su organización. Esto se registra una vez por cada buzón de correo al que un mensaje se envía, por lo que un único `ORGANIZATION_EMAIL_RECEIVED` evento puede dar lugar a varios `MAILBOX_EMAIL_DELIVERED` eventos.

Campo	Descripción
destinatario	El buzón de correo al que el mensaje se envía.
carpeta	La carpeta de buzón de correo en el que el mensaje se coloca.

`RULE_APPLIED`

Este evento se registra cuando un mensaje entrante o saliente inicia una regla de flujo de correo electrónico.

Campo	Descripción
ruleName	El nombre de la regla.
ruleType	El tipo de regla aplicada (INBOUND_RULE, OUTBOUND_RULE o MAILBOX_RULE).

Campo	Descripción
	Las reglas de entrada y salida se aplican a tu organización de Amazon WorkMail. Las reglas de buzón de correo se aplican únicamente a buzones de correo especificados. Para obtener más información, consulte Administración de flujos de correo electrónico.
ruleActions	Las acciones realizadas en función de la regla. Diferentes destinatarios del mensaje podrían tener acciones diferentes, como, por ejemplo, un correo electrónico rebotado o un correo electrónico entregado correctamente.
targetFolder	Carpeta de destino prevista para una MAILBOX_RULE `Move` o `Copy`.
targetRecipient	Destinatario de una MAILBOX_RULE `Forward` o `Redirect`.

`JOURNALING_INITIATED`

Este evento se registra cuando Amazon WorkMail envía un correo electrónico a la dirección de registro en diario especificada por el administrador de la organización. Esto solo es transmitido si se ha configurado el registro histórico de su organización. Para obtener más información, consulte Cómo usar el registro diario del correo electrónico con Amazon WorkMail.

Campo	Descripción
journalingAddress	Dirección de correo electrónico a la que se envía el mensaje de registro histórico.

`INCOMING_EMAIL_BOUNCED`

Este evento se registra cuando un mensaje entrante no se puede entregar a un destinatario. Los correos electrónicos pueden rebotar por diversas razones, como un buzón de correo de destino

lleno. El sistema registra este evento una vez por cada destinatario que provoque un correo electrónico rebotado. Por ejemplo, si un mensaje entrante se dirige a tres destinatarios y dos de ellos tienen buzones de correo completos, se registran dos INCOMING_EMAIL_BOUNCED eventos.

Campo	Descripción
bouncedRecipient	El destinatario al que Amazon WorkMail devolvió el mensaje.

`OUTGOING_EMAIL_SUBMITTED`

Este evento se registra cuando un usuario de su organización envía un mensaje de correo electrónico. Esto se registra antes de que el mensaje salga de Amazon WorkMail, por lo que este evento no indica si el correo electrónico se ha entregado correctamente.

Campo	Descripción
recipients	Los destinatarios del mensaje tal como se especifica en el remitente. Incluye todos los destinatarios en Para, CC y BCC.
remitente	La dirección de correo electrónico del usuario que envió el mensaje de correo electrónico en nombre de otro usuario. Este campo se establece únicamente cuando un mensaje de correo electrónico se envía en nombre de otro usuario.
desde	La dirección From (De), que suele ser la dirección de correo electrónico del usuario que envió el mensaje. Si el usuario envió el mensaje como otro usuario o en nombre de otro usuario, el campo devuelve la dirección de correo electrónico del usuario en cuyo nombre se ha enviado el correo electrónico, no la dirección de correo electrónico del remitente real.

Campo	Descripción
subject	El mensaje de correo electrónico.

OUTGOING_EMAIL_SENT

Este evento se registra cuando un correo electrónico saliente se ha entregado correctamente a su destinatario. Esto se registra una vez por cada destinatario correcto, por lo que un solo `OUTGOING_EMAIL_SUBMITTED` puede dar lugar a varias `OUTGOING_EMAIL_SENT` entradas.

Campo	Descripción
destinatario	El destinatario del correo electrónico que se ha enviado correctamente.
remitente	La dirección de correo electrónico del usuario que envió el mensaje de correo electrónico en nombre de otro usuario. Este campo se establece únicamente cuando un mensaje de correo electrónico se envía en nombre de otro usuario.
desde	La dirección From (De), que suele ser la dirección de correo electrónico del usuario que envió el mensaje. Si el usuario envió el mensaje como otro usuario o en nombre de otro usuario, el campo devuelve la dirección de correo electrónico del usuario en cuyo nombre se ha enviado el correo electrónico, no la dirección de correo electrónico del remitente real.
messageId	El ID de mensaje de SMTP

OUTGOING_EMAIL_BOUNCED

Este evento se registra cuando un mensaje saliente no se puede entregar a su destinatario. Los correos electrónicos pueden rebotar por diversas razones, como un buzón de correo de destino lleno. El sistema registra un rebote por cada destinatario que provoque un correo electrónico rebotado. Por ejemplo, si un mensaje saliente se dirige a tres destinatarios y dos de ellos tienen buzones de correo completos, se registran dos `OUTGOING_EMAIL_BOUNCED` eventos.

Campo	Descripción
bouncedRecipient	El destinatario por el cual el servidor de correo de destino ha rebotado el mensaje.

`DMARC_POLICY_APPLIED`

Este evento se registra cuando se aplica una política de DMARC a un correo electrónico enviado a su organización.

Campo	Descripción
desde	La dirección From (De), que suele ser la dirección de correo electrónico del usuario que envió el mensaje. Si el usuario envió el mensaje como otro usuario o en nombre de otro usuario, el campo devuelve la dirección de correo electrónico del usuario en cuyo nombre se ha enviado el correo electrónico, no la dirección de correo electrónico del remitente real.
recipients	Los destinatarios del mensaje.
policy	La política de DMARC aplicada, que indica la acción que se debe realizar en el correo electrónico cuando se produce un error en la comprobación DMARC (NONE, QUARANTIN E o REJECT). Es el mismo que el campo dmarcPolicy del evento ORGANIZAT ION_EMAIL_RECEIVED.

Supervisión de los registros WorkMail de auditoría de Amazon

Puedes usar los registros de auditoría para supervisar el acceso a los buzones de correo de tu WorkMail organización Amazon. Amazon WorkMail registra cinco tipos de eventos de auditoría y estos eventos se pueden publicar en CloudWatch Logs, Amazon S3 o Amazon Firehouse. Puede utilizar los registros de auditoría para supervisar la interacción de los usuarios con los buzones de correo de su organización, los intentos de autenticación, la evaluación de las reglas de control de acceso y realizar llamadas a los proveedores de disponibilidad a sistemas externos y supervisar los eventos con tokens de acceso personales. Para obtener información sobre la configuración de los registros de auditoría, consulteHabilitación del registro de auditoría.

En las siguientes secciones se describen los eventos de auditoría registrados por Amazon WorkMail, cuándo se transmiten los eventos y la información sobre los campos de eventos.

Registros de acceso al buzón

Los eventos de acceso a los buzones proporcionan información sobre qué acción se ha realizado (o intentado) en cada objeto del buzón. Se genera un evento de acceso al buzón por cada operación que se intenta ejecutar en un elemento o carpeta de un buzón de correo. Estos eventos son útiles para auditar el acceso a los datos del buzón.

Campo	Descripción
event_timestamp	Cuándo ocurrió el evento, en milisegundos desde la época de Unix.
request_id	El ID que identifica de forma exclusiva la solicitud.
organization_arn	El ARN de la WorkMail organización & Amazon a la que pertenece el usuario autenticado.
user_id	El ID del usuario autenticado.
impersonator_id	El ID del imitador. Está presente solo si se utilizó la función de suplantación de identidad para la solicitud.
protocolo	El protocolo utilizado. El protocolo puede ser:`AutoDiscover` ,

Campo	Descripción
	`EWSIMAP`,`WindowsOutlook` ,`ActiveSync` ,`SMTP`,`WebMail`,`IncomingEmail` , `oOutgoingEmail` .
source_ip	La dirección IP de origen de la solicitud.
user_agent	El agente de usuario que realizó la solicitud.
acción	La acción realizada sobre el objeto, que puede ser:`read`,,,`read_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	El ID del usuario propietario del objeto sobre el que se está actuando.
object_type	El tipo de objeto, que puede ser: carpeta, mensaje o adjunto.
item_id	El identificador que identifica de forma exclusiva el mensaje que es el asunto del evento o que contiene el archivo adjunto que es el asunto del evento.
folder_path	La ruta de la carpeta sobre la que se está actuando o la ruta de la carpeta que contiene el elemento sobre el que se está actuando.
folder_id	El identificador que identifica de forma exclusiva la carpeta que es el tema del evento o que contiene el objeto que es el tema del evento.

Campo	Descripción
attachment_path	La ruta de los nombres para mostrar al archivo adjunto afectado.
action_allowed	Si la acción estaba permitida. Puede ser verdadero o falso.

Registros de control de acceso

Los eventos de control de acceso se generan cada vez que se evalúa una regla de control de acceso. Estos registros son útiles para auditar los accesos prohibidos o depurar las configuraciones de control de acceso.

Campo	Descripción
event_timestamp	Cuándo ocurrió el evento, en milisegundos desde la época de Unix.
request_id	El ID que identifica de forma exclusiva la solicitud.
organization_arn	El ARN de la WorkMail organización a la que pertenece el usuario autenticado.
user_id	El ID del usuario autenticado.
impersonator_id	El ID del imitador. Está presente solo si se utilizó la función de suplantación de identidad para la solicitud.
protocolo	El protocolo utilizado, que puede ser:`AutoDiscover` ,,`EWS`,`IMAP`,`WindowsOutlook` ,`ActiveSync` , `SMTP` `WebMailIncomingEmail` , o. `OutgoingEmail`
source_ip	La dirección IP de origen de la solicitud.

Campo	Descripción
scope	El alcance de la regla, que puede ser:`AccessControl` ,`DeviceAccessControl` , `oImpersonationAccessControl` .
rule_id	El ID de la regla de control de acceso coincidente. Si no hay reglas coincidentes, el rule_id no está disponible.
access_granted	Si se permitía el acceso. Puede ser verdadero o falso.

Registros de autenticación

Los eventos de autenticación contienen información sobre los intentos de autenticación.

> **Note**
>
> Los eventos de autenticación no se generan para los eventos de autenticación a través de la WorkMail WebMail aplicación Amazon.

Campo	Descripción
event_timestamp	Cuándo ocurrió el evento, en milisegundos desde la época de Unix.
request_id	El ID que identifica de forma exclusiva la solicitud.
organization_arn	El ARN de la WorkMail organización a la que pertenece el usuario autenticado.
user_id	El ID del usuario autenticado.

Campo	Descripción
usuario	El nombre de usuario con el que se intentó la autenticación.
protocolo	El protocolo utilizado, que puede ser: `AutoDiscover EWS`,`IMAP`,`WindowsOutlook` ,`ActiveSync` ,`SMTP`,`WebMail`,`IncomingEmail` , `oOutgoingEmail` .
source_ip	La dirección IP de origen de la solicitud.
user_agent	El agente de usuario que realizó la solicitud.
method	El método de autenticación. Actualmente, solo se admite el básico.
auth_successful	Si el intento de autenticación se ha realizado correctamente. Puede ser verdadero o falso.
auth_failed_reason	El motivo del error de autenticación. Está presente solo si la autenticación ha fallado.
personal_access_token_id	El ID del token de acceso personal utilizado para la autenticación.

Registros del token de acceso personal

Se genera un evento de token de acceso personal (PAT) por cada intento de crear o eliminar un token de acceso personal. Los eventos de token de acceso personal proporcionan información sobre si los usuarios han creado correctamente los tokens de acceso personal. Los registros de los tokens de acceso personal son útiles para auditar a los usuarios finales que crean y eliminan los suyos propios PATs. El inicio de sesión del usuario con tokens de acceso personal generará eventos en los registros de autenticación existentes. Para obtener más información, consulte Registros de autenticación.

Campo	Descripción
event_timestamp	Cuándo ocurrió el evento, en milisegundos desde la época de Unix.
request_id	El ID que identifica de forma exclusiva la solicitud.
organization_arn	El ARN de la WorkMail organización a la que pertenece el usuario autenticado.
user_id	El ID del usuario autenticado.
usuario	El nombre de usuario del usuario que realizó esta acción.
protocolo	Se ejecutó el protocolo utilizado durante la acción, que puede ser: webapp
source_ip	La dirección IP de origen de la solicitud.
user_agent	El agente de usuario que realizó la solicitud.
acción	La acción del token de acceso personal, que puede ser: crear o eliminar.
nombre	El nombre del token de acceso personal.
expires_time	La fecha en la que caduca el token de acceso personal.
alcances	Los alcances de los permisos del token de acceso personal en el buzón.

Registros del proveedor de disponibilidad

Los eventos del proveedor de disponibilidad se generan para cada solicitud de disponibilidad WorkMail que Amazon realiza en tu nombre al proveedor de disponibilidad configurado. Estos eventos son útiles para depurar la configuración del proveedor de disponibilidad.

Campo	Descripción
event_timestamp	Cuándo ocurrió el evento, en milisegundos desde la época de Unix.
request_id	El ID que identifica de forma exclusiva la solicitud.
organization_arn	El ARN de la WorkMail organización a la que pertenece el usuario autenticado.
user_id	El ID del usuario autenticado.
type	El tipo de proveedor de disponibilidad que se invoca, que puede ser: `EWS` o`LAMBDA`.
Dominio	El dominio para el que se obtiene la disponibi lidad.
function_arn	El ARN de la Lambda invocada, si el tipo es LAMBDA. De lo contrario, este campo no está presente.
news_endpoint	El punto final de EWS es de tipo EWS. De lo contrario, este campo no está presente.
error_message	El mensaje que describe la causa del error. Si la solicitud se ha realizado correctamente, este campo no está presente.
availability_event_successful	Si la solicitud de disponibilidad se atendió correctamente.

Uso de CloudWatch Insights con Amazon WorkMail

Si has activado el registro de eventos por correo electrónico en la WorkMail consola de Amazon o has activado la entrega de registros de auditoría a CloudWatch Logs, puedes usar Amazon CloudWatch Logs Insights para consultar tus registros de eventos. Para obtener más información

acerca de cómo activar el registro de eventos de correo electrónico, consulte Habilitar el registro de eventos por correo electrónico. Para obtener más información sobre CloudWatch Logs Insights, consulte Analizar datos de registro con CloudWatch Logs Insights en la Guía del usuario de Amazon CloudWatch Logs.

Los siguientes ejemplos muestran cómo consultar los CloudWatch registros para detectar eventos de correo electrónico comunes. Estas consultas se ejecutan en la CloudWatch consola. Para obtener instrucciones sobre cómo ejecutar estas consultas, consulte el Tutorial: Ejecutar y modificar una consulta de ejemplo en la Guía del usuario de Amazon CloudWatch Logs.

Example Vea por qué el usuario B no recibió un correo electrónico enviado por el usuario A.

El siguiente ejemplo de código muestra cómo una consulta en un mensaje de correo electrónico enviado por un usuario saliente al usuario B, ordenados por marca de tiempo.

```
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/)
```

Esto devuelve el mensaje enviado y el ID de rastro. Utilice el ID de rastro en el siguiente ejemplo de código para consultar los registros de eventos del el mensaje enviado.

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

Devuelve el ID de mensaje de correo electrónico y los eventos de correo electrónico. `OUTGOING_EMAIL_SENT` indica que el correo electrónico se ha enviado. `OUTGOING_EMAIL_BOUNCED` indica que el correo electrónico ha rebotado. Para ver si se ha recibido el correo electrónico, consulte mediante el ID de mensaje en el siguiente ejemplo de código.

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

Esto también debe devolver el mensaje recibido, ya que tiene el mismo ID de mensaje. Utilice el ID de rastro en el siguiente ejemplo de código para consultar la entrega.

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

Devuelve la acción de entrega y las acciones de las reglas aplicables.

Example Vea todo el correo recibido de un usuario o dominio

El siguiente ejemplo de código muestra cómo consultar todo el correo recibido de un usuario especificado.

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

El siguiente ejemplo de código muestra cómo consultar todo el correo recibido de un dominio especificado.

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

Example Consulta quién envió los correos electrónicos devueltos

El siguiente ejemplo de código muestra cómo realizar consultas de correos electrónicos salientes que han rebotado, y explica también las razones de rebote.

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

En el siguiente ejemplo de código se muestra cómo consultar los correos entrantes que han sido devueltos. También devuelve las direcciones de correo electrónico de los destinatarios rechazados y los motivos del rebote.

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason,
 event.bouncedRecipient.status
```

```
| sort @timestamp desc
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

Example Consulta qué dominios envían spam

El siguiente ejemplo de código muestra cómo consultar los destinatarios de su organización que reciben spam.

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

El siguiente ejemplo de código muestra cómo consultar quién es el remitente de los mensajes de correo electrónico de spam.

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

Example Comprueba por qué se ha enviado un correo electrónico a la carpeta de correo no deseado de un destinatario

El siguiente ejemplo de código muestra cómo consultar los mensajes de correo electrónico identificados como spam, filtrados por asunto.

```
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"
```

También puede consultar mediante el ID de rastro de correo electrónico para ver todos los eventos del correo electrónico.

Example Consulta los correos electrónicos que coinciden con las reglas de flujo de correo

El siguiente ejemplo de código muestra cómo consultar los mensajes de correo electrónico que coinciden con las reglas del flujo de correo electrónico saliente.

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

El siguiente ejemplo de código muestra cómo consultar los mensajes de correo electrónico que coinciden con las reglas del flujo de correo electrónico entrante.

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

Example Vea cuántos correos electrónicos recibe o envía su organización

El siguiente ejemplo de código muestra cómo consultar el número de mensajes de correo electrónico recibido por cada destinatario de su organización.

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

El siguiente ejemplo de código muestra cómo consultar el número de mensajes de correo electrónico enviados por cada remitente en su organización.

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

Registrar llamadas a WorkMail la API de Amazon con AWS CloudTrail

Amazon WorkMail está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o una persona Servicio de AWS en Amazon WorkMail. CloudTrail captura todas las llamadas a la API de Amazon WorkMail como eventos, incluidas las llamadas desde la WorkMail consola de Amazon y las llamadas en código a Amazon WorkMail APIs. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon WorkMail. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a Amazon WorkMail, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulta la Guía AWS CloudTrail del usuario.

WorkMail Información de Amazon en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Amazon WorkMail, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos del historial de eventos. Puedes ver, buscar y descargar eventos recientes en tu Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de Amazon WorkMail, debes crear una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas WorkMail las acciones de Amazon se registran CloudTrail y se documentan en la referencia de la WorkMail API de Amazon. Por ejemplo, las llamadas a las operaciones de API de `CreateUser`, `CreateAlias` y `GetRawMessageContent` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de WorkMail registro de Amazon

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una única solicitud de cualquier origen e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etcétera. Los archivos de registro de CloudTrail no son un rastro de la pila ordenada de las llamadas a la API públicas, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `CreateUser` acción de la WorkMail API de 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"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `CreateAlias` acción de la WorkMail API de 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"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `GetRawMessageContent` acción de la 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"
}
```

Habilitar el registro de eventos por correo electrónico

Habilitas el registro de eventos de correo electrónico en la WorkMail consola de Amazon para realizar un seguimiento de los mensajes de correo electrónico de tu organización. El registro de eventos de correo electrónico utiliza un rol AWS Identity and Access Management vinculado a un servicio (SLR) para conceder permisos para publicar los registros de eventos de correo electrónico en Amazon. CloudWatch Para obtener más información sobre los roles vinculados a servicios de IAM, consulte Uso de roles vinculados a servicios para Amazon WorkMail.

En los registros de CloudWatch eventos, puedes usar herramientas de CloudWatch búsqueda y métricas para realizar un seguimiento de los mensajes y solucionar problemas relacionados con el correo electrónico. Para obtener más información sobre los registros de eventos a los que Amazon WorkMail envía CloudWatch, consultaSupervisión de los registros de eventos de WorkMail correo electrónico de Amazon. Para obtener más información sobre CloudWatch los registros, consulta la Guía del usuario de Amazon CloudWatch Logs.

Temas

- Activación del registro de eventos de correo electrónico
- Creación de un grupo de registro personalizado y un rol de IAM para el registro de eventos de correo electrónico
- Desactivación del registro de eventos de correo electrónico
- Prevención de la sustitución confusa entre servicios

Activación del registro de eventos de correo electrónico

Cuando activas el registro de eventos por correo electrónico con la configuración predeterminada, Amazon, ocurre lo WorkMail siguiente:

- Crea un rol AWS Identity and Access Management vinculado a un servicio —. `AmazonWorkMailEvents`
- Crea un grupo de CloudWatch registros —. `/aws/workmail/emailevents/`*`organization-alias`*
- Establece la retención de CloudWatch registros en 30 días.

Para activar el registro de eventos de correo electrónico

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, seleccione Configuración de registro.
4. Seleccione la pestaña de configuración del registro del flujo de correo electrónico.
5. En la sección de configuración del registro del flujo de correo electrónico, selecciona Editar.
6. Mueva el control deslizante Activar eventos de correo a la posición de encendido.
7. Realice una de las siguientes acciones:

   - (Recomendado) Elija Usar configuración predeterminada.
   - (Opcional) Desactive la opción Usar configuración predeterminada y seleccione un Grupo de registro de destino y un Rol de IAM en las listas que aparecen.

> **Note**
>
> Elija esta opción solo si ya ha creado un grupo de registro y un rol de IAM personalizado utilizando la opción AWS CLI. Para obtener más información, consulte Creación de un grupo de registro personalizado y un rol de IAM para el registro de eventos de correo electrónico.

8. Selecciona Autorizo WorkMail a Amazon a publicar registros en mi cuenta con esta configuración.
9. Seleccione Guardar.

Creación de un grupo de registro personalizado y un rol de IAM para el registro de eventos de correo electrónico

Te recomendamos que utilices la configuración predeterminada al habilitar el registro de eventos por correo electrónico para Amazon WorkMail. Si necesita una configuración de supervisión personalizada, puede utilizarla AWS CLI para crear un grupo de registro dedicado y una función de IAM personalizada para el registro de eventos de correo electrónico.

Para crear un grupo de registro y un rol de IAM personalizados para el registro de eventos de correo electrónico

1. Usa el siguiente AWS CLI comando para crear un grupo de registros en la misma AWS región que tu WorkMail organización de Amazon. Para obtener más información, consulte create-log-group en la Referencia de los comandos de AWS CLI .

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

2. Cree un archivo que contenga la siguiente política:

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

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

3. Utilice el siguiente AWS CLI comando para crear una función de IAM y adjunte este archivo como documento de política de funciones. Para obtener más información, consulte create-role en la Referencia de comandos de la AWS CLI .

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

> **Note**
>
> Si es un usuario de políticas `WorkMailFullAccess` administradas, debe incluir el término `workmail` en el nombre del rol. Esta política administrada solo le permite configurar el registro de eventos de correo electrónico con roles con `workmail` en el nombre. Para obtener más información, consulte Otorgar permisos a un usuario para transferir un rol a un AWS servicio en la Guía del usuario de IAM.

4. Cree un archivo que contenga la política del rol de IAM que creó en el paso anterior. Como mínimo, la política debe conceder permisos al rol para crear secuencias de registro e incluir eventos de registro en el grupo de registros que creó en el paso 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. Utilice el siguiente AWS CLI comando para adjuntar el archivo de política al rol de IAM. Para obtener más información, consulte put-role-policy en la Referencia de los comandos de AWS CLI .

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

Desactivación del registro de eventos de correo electrónico

Desactiva el registro de eventos por correo electrónico desde la WorkMail consola de Amazon. Si ya no necesitas usar el registro de eventos por correo electrónico, te recomendamos que elimines también el grupo de CloudWatch registro relacionado y la función vinculada al servicio. Para obtener más información, consulte Eliminar un rol vinculado a un servicio para Amazon WorkMail.

Para desactivar el registro de eventos de correo electrónico

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, seleccione Supervisión.
4. En la sección Configuración, elija Editar.
5. Mueva el control deslizante Habilitar eventos de correo a la posición desactivado.
6. Seleccione Guardar.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puedes producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama).

El servicio de llamadas puede manipularse para utilizar sus permisos y utilizar los recursos de otro cliente a los que, de otro modo, no tendría permiso para acceder.

Para evitarlo, AWS proporciona herramientas que te ayudan a proteger los datos de todos los servicios cuyos directores de servicio tengan acceso a los recursos de tu cuenta.

Recomendamos utilizar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que CloudWatch Logs y Amazon S3 conceden a los servicios que generan registros. Si usa ambas claves de contexto de condición global, los valores deben usar el mismo ID de cuenta cuando se usen en la misma declaración de política.

Los valores de `aws:SourceArn` deben ser los ARNs de las fuentes de entrega que generan los registros.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con comodines (`*`) para las partes desconocidas del ARN.

Habilitación del registro de auditoría

Puedes usar los registros de auditoría para recopilar información detallada sobre el uso que haces en tu WorkMail organización de Amazon. Los registros de auditoría se pueden utilizar para supervisar el acceso de los usuarios a los buzones de correo, realizar auditorías en busca de actividades sospechosas y depurar las configuraciones de los proveedores de control de acceso y disponibilidad.

> **Note**
>
> La política AmazonWorkMailFullAccessadministrada no incluye todos los permisos necesarios para administrar las entregas de registros. Si utiliza esta política para administrar WorkMail, asegúrese de que el principal (por ejemplo, el rol asumido) utilizado para configurar las entregas de registros también tenga todos los permisos necesarios.

Amazon WorkMail admite tres destinos de entrega para los registros de auditoría: CloudWatch Logs, Amazon S3 y Amazon Data Firehose. Para obtener más información, consulte Registros que requieren permisos adicionales [V2] en la Guía del usuario de Amazon CloudWatch Logs.

Además de los permisos enumerados en Registro que requiere permisos adicionales [V2], Amazon WorkMail requiere un permiso adicional para configurar la entrega de registros:`workmail:AllowVendedLogDeliveryForResource`.

La entrega de un registro funcional consta de tres elementos:

- DeliverySource, un objeto lógico que representa el recurso o los recursos que envían los registros. Para Amazon WorkMail, es la WorkMail Organización Amazon.
- Un DeliveryDestination, que es un objeto lógico que representa el destino de entrega real.
- Una entrega, que conecta una fuente de entrega con el destino de entrega.

Para configurar la entrega de registros entre Amazon WorkMail y un destino, puedes hacer lo siguiente:

- Crea una fuente de entrega con PutDeliverySource.
- Cree un destino de entrega con PutDeliveryDestination.
- Si vas a entregar registros entre cuentas, debes utilizarlos PutDeliveryDestinationPolicyen la cuenta de destino para asignar una política de IAM al destino. Esta política autoriza la creación de una entrega desde la fuente de entrega de la cuenta A hasta el destino de la entrega de la cuenta B.
- Cree una entrega combinando exactamente una fuente de entrega y un destino de entrega mediante CreateDelivery.

En las siguientes secciones se proporcionan los detalles de los permisos que debe tener al iniciar sesión para configurar la entrega de registros a cada tipo de destino. Estos permisos se pueden conceder a un rol de IAM con el que hayas iniciado sesión.

> **Important**
>
> Es su responsabilidad eliminar los recursos de entrega de registros después de eliminar el recurso generador de registros.

Para eliminar los recursos de entrega de registros después de eliminar el recurso generador de registros, sigue estos pasos.

1. Elimine la entrega mediante la DeleteDeliveryoperación.

2. Elimine la DeliverySourcemediante la DeleteDeliverySourceoperación.
3. Si el DeliveryDestinationelemento asociado al DeliverySourceque acaba de eliminar se usa solo para este DeliverySourcepropósito específico, puede eliminarlo mediante la DeleteDeliveryDestinationsoperación.

Configuración del registro de auditoría mediante la WorkMail consola de Amazon

Puedes configurar el registro de auditoría en la WorkMail consola de Amazon:

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y seleccione una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. Seleccione la configuración de registro.
4. Seleccione la pestaña Configuración del registro de auditoría.
5. Configure las entregas para el tipo de registro requerido mediante el widget correspondiente.
6. Seleccione Guardar.

Los registros se envían a CloudWatch Logs

Permisos de usuario

Para habilitar el envío de CloudWatch registros a Logs, debe iniciar sesión con los siguientes permisos.

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

Política de recursos del grupo de registro

El grupo de registro al que se envían los registros debe tener una política de recursos que incluya determinados permisos. Si el grupo de registros actualmente no tiene una política de recursos y el usuario que configura el registro tiene los `logs:PutResourcePolicy` `logs:DescribeLogGroups` permisos y los permisos para el grupo de registros, crea AWS automáticamente la siguiente política para él cuando comience a enviar los CloudWatch registros a Logs. `logs:DescribeResourcePolicies`

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

Consideraciones de límite de tamaño de la política de recursos del grupo de registro

Estos servicios deben enumerar cada grupo de registros al que envían registros en la política de recursos. CloudWatch Las políticas de recursos de registros están limitadas a 5.120 caracteres. Un servicio que envía registros a un gran número de grupos de registro puede alcanzar este límite.

Para mitigar esta situación, CloudWatch Logs supervisa el tamaño de las políticas de recursos utilizadas por el servicio que envía los registros. Cuando detecta que una política se acerca al límite de tamaño de 5.120 caracteres, CloudWatch Logs activa automáticamente `/aws/vendedlogs/*` la política de recursos de ese servicio. Puede comenzar a utilizar grupos de registro con nombres que comiencen por `/aws/vendedlogs/` como los destinos de los registros de estos servicios.

Registros enviados a Amazon S3

Permisos de usuario

Para habilitar el envío de registros a Amazon S3, debe iniciar sesión con los siguientes permisos.

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

El bucket de S3 al que se envían los registros debe tener una política de recursos que incluya determinados permisos. Si el bucket no tiene actualmente una política de recursos y el usuario que configura el registro tiene los `S3:PutBucketPolicy` permisos `S3:GetBucketPolicy` y para el bucket, creará AWS automáticamente la siguiente política para él cuando comience a enviar los registros a 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:*"
                    ]
                }
            }
        }
    ]
}
```

En la política anterior, para`aws:SourceAccount`, especifique la lista de cuentas IDs para las que se van a entregar los registros a este depósito. Para`aws:SourceArn`, especifique la lista ARNs del recurso que genera los registros, en el formulario`arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`.

Si el depósito tiene una política de recursos, pero esa política no contiene la declaración que se muestra en la política anterior y el usuario que configura el registro tiene `S3:PutBucketPolicy` los permisos `S3:GetBucketPolicy` y los permisos para el depósito, esa declaración se adjunta a la política de recursos del depósito.

> **Note**
>
> En algunos casos, es posible que veas `AccessDenied` errores al AWS CloudTrail indicar si no se ha concedido el `s3:ListBucket` permiso. `delivery.logs.amazonaws.com` Para evitar estos errores en tus CloudTrail registros, debes conceder el `s3:ListBucket` permiso a`delivery.logs.amazonaws.com`. También debe incluir los `Condition` parámetros que se muestran con el `s3:GetBucketAcl` permiso establecido en la política de bucket anterior. Para simplificarlo, en lugar de crear uno nuevo`Statement`, puedes actualizar directamente el `AWSLogDeliveryAclCheck` futuro`“Action”: [“s3:GetBucketAcl”, “s3:ListBucket”]`.

Uso de cifrado del servidor del bucket de Amazon S3

Puede proteger los datos de su bucket de Amazon S3 habilitando el cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3) o el cifrado del lado del servidor con una

clave almacenada en (SSE-KMS). AWS KMS AWS Key Management Service Para obtener más información, consulte Protección de los datos con el cifrado del servidor.

Si elige SSE-S3, no se requiere ninguna configuración adicional. Amazon S3 se encarga de la clave de cifrado.

> **Warning**
>
> Si elige SSE-KMS, debe usar una clave administrada por el cliente, ya que no se admite el uso de una en este escenario. Clave administrada de AWS Si configuras el cifrado con una clave AWS gestionada, los registros se entregarán en un formato ilegible.

Cuando utilizas una AWS KMS clave gestionada por el cliente, puedes especificar el nombre de recurso de Amazon (ARN) de la clave gestionada por el cliente al activar el cifrado de buckets. Añada lo siguiente a la política de claves de su clave gestionada por el cliente (no a la política de bucket de su bucket de S3), de modo que la cuenta de entrega de registros pueda escribir en su bucket de S3.

Si eliges SSE-KMS, debes usar una clave administrada por el cliente, ya que no se admite el uso de una clave AWS administrada en este escenario. Cuando utilizas una AWS KMS clave gestionada por el cliente, puedes especificar el nombre de recurso de Amazon (ARN) de la clave gestionada por el cliente al activar el cifrado de buckets. Añada lo siguiente a la política de claves de su clave gestionada por el cliente (no a la política de bucket de su bucket de S3), de modo que la cuenta de entrega de registros pueda escribir en su bucket de 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:*"
            ]
        }
    }
}
```

Para elloaws:SourceAccount, especifique la lista de cuentas IDs para las que se van a entregar los registros a este depósito. Paraaws:SourceArn, especifique la lista ARNs del recurso que genera los registros, en el formularioarn:aws:logs:*source-region*:*source-account-id*:*.

Registros enviados a Firehose

Permisos de usuario

Para habilitar el envío de registros a Firehose, debe iniciar sesión con los siguientes permisos.

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

Roles de IAM utilizados para permisos de recursos

Como Firehose no usa políticas de recursos, AWS usa roles de IAM al configurar estos registros para enviarlos a Firehose. AWS crea un rol vinculado a un servicio denominado AWSServiceRoleForLogDelivery. Esta función vinculada al servicio incluye los siguientes permisos.

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

Esta función vinculada al servicio concede permisos para todas las transmisiones de entrega de Firehose que tengan la `LogDeliveryEnabled` etiqueta establecida en. `true` AWS asigna esta etiqueta al flujo de entrega de destino cuando configuras el registro.

Este rol vinculado a un servicio también tiene una política de confianza que permite que la entidad principal de servicio `delivery.logs.amazonaws.com` asuma el rol vinculado al servicio necesario. Esta política de confianza es la siguiente:

```
{
```

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

Permisos específicos de la consola

Además de los permisos enumerados en las secciones anteriores, si va a configurar la entrega de registros mediante la consola en lugar de mediante la consola APIs, también necesitará los siguientes permisos:

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

Validación de conformidad para Amazon WorkMail

Los auditores externos evalúan la seguridad y el cumplimiento de Amazon WorkMail como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, ISO y C5.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de conformidad específicos, consulte Servicios de AWS incluidos en el ámbito de aplicación por programa de conformidad. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Tu responsabilidad de conformidad al utilizar Amazon WorkMail viene determinada por la confidencialidad de tus datos, los objetivos de cumplimiento de tu empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- AWS Recursos de conformidad: esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- AWS Config— Este AWS servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en Amazon WorkMail

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las

zonas de disponibilidad, puedes diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Amazon WorkMail ofrece varias funciones que ayudan a respaldar sus necesidades de respaldo y resiliencia de datos.

Seguridad de la infraestructura en Amazon WorkMail

> **Note**
>
> Amazon WorkMail dejó de ofrecer soporte para las versiones 1.0 y 1.1 de Transport Layer Security (TLS). Si utiliza TLS 1.0 o 1.1, debe actualizar la versión de TLS a la 1.2. Para obtener más información, consulte TLS 1.2 para convertirse en el nivel mínimo de protocolo TLS para todos los puntos de enlace de las API de AWS.

Como servicio gestionado, Amazon WorkMail está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utilizas las llamadas a la API AWS publicadas para acceder a Amazon WorkMail a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Cómo empezar con Amazon WorkMail

Una vez que hayas completado elRequisitos previos, estarás listo para empezar a utilizar Amazon WorkMail. Para obtener más información, consulte Cómo empezar con Amazon WorkMail.

Puede obtener más información sobre la migración de los buzones de correo existentes a Amazon WorkMail, la interoperabilidad con Microsoft Exchange y WorkMail las cuotas de Amazon en las siguientes secciones.

Temas

Cómo empezar con Amazon WorkMail

Tanto si eres un WorkMail usuario nuevo de Amazon como si ya eres usuario de Amazon WorkSpaces, sigue estos pasos para empezar a utilizar Amazon WorkMail .

> **Note**
>
> Complete los Requisitos previos antes de comenzar a utilizar el servicio.

Temas

Paso 1: inicia sesión en la WorkMail consola de Amazon

Debes iniciar sesión en la WorkMail consola de Amazon para poder añadir usuarios y gestionar sus cuentas y buzones.

Para iniciar sesión en la WorkMail consola de Amazon

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.
2. Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información sobre las regiones, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.

Paso 2: Configura tu WorkMail sitio de Amazon

1. Tras iniciar sesión en la WorkMail consola de Amazon, configuras tu organización y añades un dominio. Te recomendamos usar un dominio dedicado para tu WorkMail organización de Amazon. Para obtener más información, consulte Creación de una organización y Adición de un dominio.
2. (Opcional) Puedes optar por utilizar un dominio de prueba gratuito proporcionado por Amazon WorkMail. Si decide hacerlo, vaya al paso 4.

> **Note**
>
> Los dominios de prueba utilizan este formato: *alias* .awsapps.com. A medida que avance, recuerde que solo debe utilizar dominios de prueba para realizar pruebas. No utilice un dominio de prueba para un entorno de producción. Además, debes tener al menos un usuario habilitado en tu WorkMail organización de Amazon. Si no tiene un usuario habilitado, el dominio podría quedar disponible para que otros clientes lo registren y lo utilicen.

3. Si utiliza un dominio externo, verifíquelo añadiendo los registros de texto (TXT) y de intercambiador de correo (MX) apropiados a su servicio de Sistema de nombres de dominio (DNS). Los registros TXT le permiten introducir notas en el DNS. Los registros MX especifican los servidores de correo entrante. Asegúrese de establecer su dominio como predeterminado para su organización. Para obtener más información, consulte Verificación de dominios y Elección del dominio predeterminado.
4. Crea nuevos usuarios o habilita los usuarios de tu directorio existentes para Amazon WorkMail. Para obtener más información, consulte Agregar un usuario.
5. (Opcional) Si ya tienes buzones de Microsoft Exchange, mírgalos a Amazon WorkMail. Para obtener más información, consulte Migración a Amazon WorkMail.

Cuando hayas terminado de configurar tu WorkMail sitio de Amazon, podrás acceder a Amazon WorkMail mediante la URL de la aplicación web.

Para localizar la URL de la aplicación WorkMail web de Amazon

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. Para ello, abra la lista Seleccionar una región situada a la derecha del cuadro de búsqueda y elija la región deseada. Para obtener más información, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.

   Aparece la página Configuración de la organización, que muestra el URL en Inicio de sesión de usuario. Luego, URLs complete este formulario: https://*alias*.awsapps.com/mail.

Paso 3: Configurar el acceso de los WorkMail usuarios de Amazon

Elige una de las siguientes opciones para configurar el acceso de los WorkMail usuarios de Amazon:

- Configurar el acceso de los usuarios desde un cliente de escritorio existente con el cliente de Microsoft Outlook. Para obtener más información, consulta Conectar Microsoft Outlook a tu WorkMail cuenta de Amazon.
- Configure el acceso de usuario desde un dispositivo móvil, como Kindle, Android, iPad o iPhone. Para obtener más información, consulte Configuración para utilizar un dispositivo móvil.

- Para configurar el acceso de usuario, utilice cualquier software cliente compatible con el protocolo de acceso al correo de Internet (IMAP). Para obtener más información, consulta Conectar clientes IMAP a tu WorkMail cuenta de Amazon.

Más recursos

- Migración a Amazon WorkMail
- Interoperabilidad entre Amazon WorkMail y Microsoft Exchange
- WorkMail Cuotas de Amazon

Migración a Amazon WorkMail

Puedes migrar a Amazon WorkMail desde Microsoft Exchange, Microsoft Office 365, G Suite Basic (anteriormente Google Apps for Work) y otras plataformas si trabajas con uno de nuestros socios. Para obtener más información sobre nuestros socios, consulta Amazon WorkMail Features.

Temas

- Paso 1: Crear o habilitar usuarios en Amazon WorkMail
- Paso 2: migrar a Amazon WorkMail
- Paso 3: completar la migración a Amazon WorkMail

Paso 1: Crear o habilitar usuarios en Amazon WorkMail

Antes de migrar tus usuarios, debes añadirlos WorkMail a Amazon para aprovisionar sus buzones de correo. Para obtener más información, consulte Agregar un usuario.

Paso 2: migrar a Amazon WorkMail

Puedes trabajar con cualquier socio de AWS migración para migrar a Amazon WorkMail. Para obtener información sobre estos proveedores, consulta las WorkMailcaracterísticas de Amazon.

Para migrar tus buzones de correo, crea un WorkMail usuario exclusivo de Amazon que actúe como administrador de la migración. El siguiente procedimiento concede permiso a dicho usuario para acceder a todos los buzones de correo de su organización.

Para crear un administrador de migración

1. Realice una de las siguientes acciones:
   - En la WorkMail consola de Amazon, crea un nuevo usuario para que actúe como administrador de la migración. Para obtener más información, consulte Agregar un usuario.
   - En Active Directory, cree un nuevo usuario para que actúe como administrador de migración y, a continuación, habilite el usuario para Amazon WorkMail. Para obtener más información, consulte Habilitar usuarios.
2. En el panel de navegación de la WorkMail consola de Amazon, selecciona Organizations y, a continuación, elige el nombre de tu organización.
3. Elija Configuración de la organización, Migración y, a continuación, Editar.
4. Mueva el control deslizante Migración habilitada a la posición activado.
5. Abra el Administrador de migración y seleccione un usuario.
6. Seleccione Save.

Paso 3: completar la migración a Amazon WorkMail

Después de migrar tus cuentas de correo electrónico a Amazon WorkMail, puedes verificar tus registros de DNS y configurar tus clientes móviles y de escritorio.

Para completar la migración a Amazon WorkMail

1. Comprueba que todos los registros DNS estén actualizados y que apunten a Amazon WorkMail. Para obtener más información sobre los registros de DNS, consulte Adición de un dominio.

   > **Note**
   >
   > El proceso de actualización de los registros DNS puede durar varias horas. Si aparece algún elemento nuevo en el buzón de correo de origen mientras se cambian los registros MX, ejecute la herramienta de migración de nuevo para migrar los elementos nuevos después de que se actualicen los registros de DNS.

2. Para obtener más información sobre cómo configurar tus clientes de escritorio o móviles para usar Amazon WorkMail, consulta Conectar Microsoft Outlook a tu WorkMail cuenta de Amazon en la Guía del WorkMail usuario de Amazon.

Interoperabilidad entre Amazon WorkMail y Microsoft Exchange

La interoperabilidad entre Amazon WorkMail y Microsoft Exchange Server le permite minimizar las interrupciones para sus usuarios al migrar los buzones a Amazon WorkMail o utilizar Amazon WorkMail para un subconjunto de sus buzones corporativos.

Esta interoperabilidad le permite utilizar el mismo dominio corporativo para los buzones de correo de los dos entornos. De este modo, sus usuarios podrán programar reuniones compartiendo de forma bidireccional la información sobre el estado libre/ocupado del calendario.

Requisitos previos

Antes de habilitar la interoperabilidad con Microsoft Exchange, haga lo siguiente:

- Asegúrese de tener al menos un usuario habilitado para Amazon. WorkMail Esto es necesario para configurar los ajustes de disponibilidad de Microsoft Exchange. Para habilitar un usuario, siga los pasos en Habilitar el direccionamiento de correo electrónico para un usuario.
- Configure un conector de Active Directory (AD). La configuración de un conector AD con su directorio en las instalaciones permite a los usuarios seguir utilizando sus credenciales corporativas existentes. Para obtener más información, consulte Crear un conector AD e integrar Amazon WorkMail con su directorio local.
- Configura tu WorkMail organización de Amazon. Crea una WorkMail organización de Amazon que utilice el AD Connector que configuraste.
- Añade tus dominios corporativos a tu WorkMail organización de Amazon y, a continuación, verifícalos en la WorkMail consola de Amazon. De lo contrario, los correos electrónicos enviados a este alias rebotarán. Para obtener más información, consulte Uso de dominios.
- Migre los buzones de correo a Amazon WorkMail. Permita a los usuarios aprovisionar y migrar los buzones de su entorno local a Amazon. WorkMail Para obtener más información, consulte Habilitar usuarios existentes y consulte Migración a Amazon WorkMail.

  > **Note**
  >
  > No actualice los registros de DNS para que apunten a Amazon WorkMail. De este modo, se asegura de que Microsoft Exchange sigue siendo el servidor principal para los correos entrantes siempre que desee mantener la interoperabilidad entre los dos entornos.

- Asegúrese de que los nombres principales de los usuarios (UPNs) de Active Directory coincidan con las direcciones SMTP principales de los usuarios.

Amazon WorkMail realiza solicitudes HTTPS a la URL de los servicios web de Exchange (EWS) de Microsoft Exchange para obtener información sobre las horas libres y ocupadas del calendario.

En el caso de los proveedores de disponibilidad basados en EWS, Amazon WorkMail realiza solicitudes HTTPS a la URL de los servicios web de Exchange (EWS) de Microsoft Exchange para obtener información sobre las horas libres y ocupadas del calendario. Por lo tanto, los siguientes requisitos previos solo se aplican a los proveedores de disponibilidad basados en EWS.

- Asegúrese de que los ajustes pertinentes del cortafuegos están configurados para permitir el acceso desde Internet. El puerto predeterminado para las solicitudes HTTPS es el puerto 443.
- Amazon solo WorkMail puede realizar solicitudes HTTPS satisfactorias a la URL de EWS en Microsoft Exchange si hay un certificado firmado por una autoridad de certificación (CA) válida disponible en su entorno de Microsoft Exchange. Para obtener más información, consulte Creación de una solicitud de certificado de servidor Exchange para una autoridad de certificación en el sitio web de documentación de Microsoft Exchange.
- Debe habilitar Autenticación básica para EWS en Microsoft Exchange. Para obtener más información, consulte Directorios virtuales: Exchange 2013 en el blog Microsoft MVP Award Program.

Adición de dominios y habilitación de buzones de correo

Añade tus dominios corporativos a Amazon WorkMail para que se puedan usar en las direcciones de correo electrónico. Asegúrese de que los dominios añadidos a Amazon WorkMail estén verificados y, a continuación, permita a los usuarios y grupos aprovisionar buzones de correo en Amazon WorkMail. Los recursos no se pueden habilitar en Amazon en WorkMail el modo de interoperabilidad y se deben volver a crear en Amazon WorkMail después de deshabilitar el modo de interoperabilidad. Sin embargo, puede utilizarlos para programar reuniones mientras está en el modo de interoperabilidad. Los recursos de Microsoft Exchange siempre se muestran en la pestaña Usuarios de Amazon WorkMail.

- Para obtener más información, consulte Añadir dominios, Habilitar usuarios existentes y Habilitar un grupo existente.

> **Note**
>
> Para garantizar la interoperabilidad con Microsoft Exchange, no actualice los registros de DNS para que apunten a los WorkMail registros de Amazon. Microsoft Exchange sigue siendo el servidor principal para los correos electrónicos entrantes siempre que usted desee mantener la interoperabilidad entre los dos entornos.

Habilitación de la interoperabilidad

Si no has creado una WorkMail organización de Amazon, puedes usar la API pública para crear una nueva WorkMail organización con el modo de interoperabilidad activado.

Si ya tiene una WorkMail organización de Amazon con un conector AD Connector vinculado a Active Directory y también tiene Microsoft Exchange, póngase en contacto con AWS Support para obtener ayuda sobre cómo habilitar la interoperabilidad de Microsoft Exchange para una WorkMail organización de Amazon existente.

Crear cuentas de servicio en Microsoft Exchange y Amazon WorkMail

> **Note**
>
> No es necesario crear una cuenta de servicio en Exchange cuando Exchange no se utiliza como back-end para el proveedor de disponibilidad personalizado.

Para acceder a la 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 información del calendario de otros usuarios de Exchange. El acceso se otorga de forma predeterminada, por lo que no se necesitan permisos especiales.

Del mismo modo, la cuenta de WorkMail servicio de Amazon es cualquier usuario de Amazon WorkMail que tenga acceso a la información de horarios libres y ocupados de otros usuarios de Amazon WorkMail . Este acceso también se otorga de forma predeterminada. Debe crear el WorkMail usuario de Amazon en su directorio local y, a continuación WorkMail, habilitar ese usuario para Amazon para integrar Amazon WorkMail con AD Connector en su directorio.

Limitaciones en modo de interoperabilidad

Si su organización se encuentra en modo de interoperabilidad, debe utilizar el centro de administración de Exchange para administrar todos los usuarios, grupos y recursos. Para habilitar WorkMail los usuarios y grupos de Amazon, usa AWS Management Console. Para obtener más información, consulte Habilitación de usuarios existentes y Habilitación de un grupo existente.

Al habilitar un usuario o grupo para Amazon WorkMail, no puedes editar las direcciones de correo electrónico ni los alias de esos usuarios y grupos. Estos datos también se deben configurar a través del admincenter de Exchange. Amazon WorkMail sincroniza los cambios del directorio cada cuatro horas.

Los recursos no se pueden crear ni habilitar en Amazon WorkMail en modo de interoperabilidad. Sin embargo, todos tus recursos de Exchange están disponibles en la libreta de WorkMail direcciones de Amazon y se pueden usar para programar reuniones como de costumbre.

Configurar los ajustes de disponibilidad en Amazon WorkMail

Configura los ajustes de disponibilidad en Amazon WorkMail para permitir la consulta de sistemas externos, ofrecer funciones de calendario y obtener free/busy information. Amazon WorkMail supports two modes of obtaining free/busy información del calendario desde un sistema remoto:

- Servicios web de Exchange (EWS): en esta configuración, Amazon WorkMail consultará la información de disponibilidad en un servidor de Exchange u otra WorkMail organización mediante el protocolo EWS. Esta es la configuración más sencilla pero requiere que el punto de conexión de EWS del servidor Exchange sea accesible a través de internet pública.
- Proveedor de disponibilidad personalizado (CAP): en esta configuración, un administrador puede configurar una función de Lambda de AWS para obtener información sobre disponibilidad de los usuarios para un dominio de correo electrónico determinado. En función de la plataforma de servidor de correo electrónico, el uso de CAP con Amazon WorkMail ofrece las siguientes ventajas:
  - Obtenga la disponibilidad de los usuarios a través del EWS interno sin necesidad de abrir su firewall WorkMail.
  - Obtención de disponibilidad de usuarios desde sistemas que no sean Exchange o EWS, como Google Workspace (antes conocido como G Suite).

Temas

Configuración de un proveedor de disponibilidad basado en EWS

Para configurar un proveedor de disponibilidad basado en EWS en la consola, complete el siguiente procedimiento:

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. Para ello, abra la lista Seleccionar una región situada a la derecha del cuadro de búsqueda y elija la región deseada. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de una organización.
3. En el panel de navegación, elija Configuración de la organización y, a continuación, elija la pestaña Interoperabilidad.
4. Elija Añadir configuración de disponibilidad y, a continuación, introduzca la siguiente información:
   - Tipo: seleccione EWS.
   - Dominio: el dominio para el que WorkMail se intentará consultar la información de disponibilidad mediante esta configuración.
   - URL de EWS: Amazon WorkMail consultará esta URL al punto de conexión de EWS. Consulte la sección Obtención del URL de EWS de esta guía.
   - Dirección de correo electrónico del usuario: la dirección de correo electrónico del usuario que WorkMail utilizará para autenticarse en el punto final de EWS.
   - Contraseña: la contraseña que WorkMail se utilizará para autenticarse en el punto final de EWS.
5. Seleccione Save.

Obtención del URL de EWS

Para obtener el URL de EWS para Exchange utilizando Microsoft Outlook, complete el siguiente procedimiento:

1. Inicie sesión en Microsoft Outlook en Windows para el usuario que desee en el entorno Exchange.
2. Mantenga pulsada la tecla Ctrl y abra el menú contextual (botón derecho) en el icono de Microsoft Outlook en la barra de tareas.
3. Elija Probar correo electrónico AutoConfiguration.
4. Escriba la contraseña y dirección de correo electrónico del usuario de Microsoft Exchange y elija Test.
5. En la ventana Results, copie el valor de Availability Service URL.

Para obtener la URL de EWS para el intercambio PowerShell, ejecute el PowerShell siguiente comando en la línea de comandos:

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

Para obtener la URL de EWS de Amazon WorkMail, primero busque el dominio de EWS en los WorkMail puntos de destino y las cuotas de Amazon. Introduzca el URL de EWS - `https://"EWS domain"/EWS/Exchange.asmx` y sustituya “dominio de EWS” por su dominio de EWS.

Configuración de un proveedor de disponibilidad personalizado

Para configurar un Proveedor de Disponibilidad Personalizado (CAP), complete el siguiente procedimiento:

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. Para ello, abra la lista Seleccionar una región situada a la derecha del cuadro de búsqueda y elija la región deseada.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de una organización.
3. En el panel de navegación, elija Configuración de la organización y, a continuación, elija Interoperabilidad.
4. Elija Añadir configuración de disponibilidad y, a continuación, introduzca la siguiente información:

   - Tipo: seleccione Lambda de CAP.
   - Dominio: el dominio para el que WorkMail se intentará consultar la información de disponibilidad mediante esta configuración.
   - ARN: el ARN de la función de Lambda que proporcionará la información de disponibilidad.

Para crear una función de Lambda de CAP, consulte Creación de una función de Lambda de proveedor de disponibilidad personalizada.

Creación de una función de Lambda de proveedor de disponibilidad personalizada

Los proveedores de disponibilidad personalizados (CAPs) se configuran con un protocolo de solicitud y respuesta basado en JSON escrito en un esquema JSON bien definido. Una función de Lambda analizará la solicitud y proporcionará una respuesta válida.

Temas

- Elementos de solicitud y respuesta
- Concesión de acceso
- Ejemplo de Amazon WorkMail utilizando una función CAP Lambda

Elementos de solicitud y respuesta

Elementos de la solicitud

El siguiente es un ejemplo de solicitud que se utiliza para configurar un CAP para un WorkMail usuario de 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 solicitud consta de tres secciones: requester, mailboxes, y window. Estas se describen en las correspondientes secciones Solicitante, Buzones y Ventana de esta guía.

Solicitante

La sección del solicitante proporciona información sobre el usuario que realizó la solicitud original a Amazon WorkMail. CAPs utilice esta información para cambiar el comportamiento del proveedor. Por ejemplo, estos datos se pueden utilizar para suplantar al mismo usuario en el proveedor de disponibilidad de backend o se pueden omitir ciertos detalles de la respuesta.

Campo	Descripción	Obligatorio
`Email`	La dirección de correo electrónico principal del solicitante.	Sí
`Username`	El nombre de usuario del solicitante.	Sí
`Organization`	El ID de organización del solicitante.	Sí
`UserID`	El ID del solicitante.	Sí
`Origin`	La dirección remota de la solicitud.	No
`Bearer`	Reservado para uso futuro.	No

Buzones

La sección mailboxes contiene una lista separada por comas de las direcciones de correo electrónico de los usuarios para los que se solicita la información de disponibilidad.

Ventana

La sección window contiene la ventana temporal para la que se solicita la información de disponibilidad. Tanto `startDate` como `endDate` se especifican en UTC y se formatean según RFC 3339. No se espera que los eventos se trunquen. En otras palabras, si un evento comienza antes de la `StartDate` definida, se utiliza el inicio original.

Elementos de respuesta

Amazon WorkMail esperará 25 segundos para obtener una respuesta de la función CAP Lambda. Transcurridos 25 segundos, Amazon WorkMail asumirá que la función ha fallado y generará errores en los buzones de correo asociados en la GetUserAvailability respuesta de EWS. Esto no provocará un error en toda la GetUserAvailability operación.

A continuación se muestra un ejemplo de respuesta de la configuración definida al principio de esta sección:

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

La respuesta se compone de una única sección, mailboxes, que consiste en una lista de buzones de correo. Cada buzón de correo cuya disponibilidad se obtenga de forma satisfactoria consta de tres secciones: mailbox, events y workinghours. Si el proveedor de disponibilidad no ha podido obtener información de disponibilidad para un buzón de correo, la sección consta de dos secciones: mailbox y error. Estas se describen en las correspondientes secciones Buzón de correo, Eventos, Horario de trabajo, Zona horaria, Periodos de trabajo y Error de esta guía.

Buzón de correo

La sección mailbox es la dirección de correo electrónico del usuario que se encuentra en la sección mailboxes de la solicitud.

Eventos

La sección events es una lista de eventos que se producen en la ventana solicitada. Cada evento se define con los siguientes parámetros:

Campo	Descripción	Obligatorio
`startTime`	La hora de inicio del evento en UTC y formateada según RFC 3339.	Sí

Campo	Descripción	Obligatorio
`endTime`	La hora de finalización del evento en UTC y formateada según RFC 3339.	Sí
`busyType`	El tipo de ocupado del evento. Puede ser `Busy`, `Free` o `Tentative` .	Sí
`details`	Los detalles del evento.	No
`details.subject`	El asunto del evento.	Sí
`details.location`	La ubicación del evento.	Sí
`details.instanceType`	El tipo de instancia del evento. Puede ser `Single_Instance` , `Recurring_Instance` o `Exception` .	Sí
`details.isMeeting`	Un booleano para indicar si el evento tiene asistentes.	Sí
`details.isReminderSet`	Un booleano para indicar si el evento tiene un recordatorio establecido.	Sí
`details.isPrivate`	Un booleano para indicar si el evento está configurado como privado.	Sí

Horario de trabajo

La sección workingHours contiene información sobre el horario de trabajo del propietario del buzón de correo. Contiene dos secciones: timezone y workingPeriods.

Zona horaria

La subsección timezone describe la zona horaria del propietario del buzón de correo. Es importante representar correctamente el horario de trabajo del usuario cuando el solicitante trabaje en una zona horaria diferente. El proveedor de disponibilidad debe describir explícitamente la zona horaria en vez de utilizar un nombre. El uso de la descripción estandarizada de zona horaria ayuda a evitar discordancias de zonas horarias.

Campo	Descripción	Obligatorio
`name`	El nombre de la zona horaria.	Sí
`bias`	El desfase predeterminado respecto a GMT en minutos.	Sí
`standardTime`	El inicio del horario estándar para la zona horaria especific ada.	No
`daylightTime`	El inicio del horario de verano para la zona horaria especific ada.	No

Debe definir tanto `standardTime` como `daylightTime`, u omitir ambos. Los campos del objeto `standardTime` y `daylightTime` son:

Campo	Descripción	Valores permitidos
`offset`	El desfase relativo al desfase predeterminado en minutos.	N/D
`time`	La hora en que se produce la transición entre horario estándar y horario de verano, especificada como `hh:mm:ss`.	N/D

Campo	Descripción	Valores permitidos
`month`	El mes en el que se produce la transición entre horario estándar y horario de verano.	`JAN`,`FEB`, `MAR`, `APR`, `JUN`, `JUL`, `AUG`, `SEP`, `OCT`, `NOV`, `DEC`
`week`	La semana dentro del mes especificado en que se produce la transición entre horario estándar y horario de verano.	`FIRST`, `SECOND`, `THIRD`, `FOURTH`, `LAST`
`dayOfWeek`	El día dentro de la semana especificada en que se produce la transición entre horario estándar y horario de verano.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Periodos de trabajo

La sección workingPeriods contiene uno o más objetos de períodos de trabajo. Cada período define un inicio y fin de la jornada laboral para uno o más días.

Campo	Descripción	Valores permitidos
`startMinutes`	El inicio de la jornada laboral en minutos a partir de medianoche.	N/D
`endMinutes`	El final de la jornada laboral en minutos a partir de medianoche.	N/D
`days`	Los días en que se aplica este período.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Error

El campo error puede contener mensajes de error arbitrarios. En la siguiente tabla se muestra una asignación de códigos bien conocidos a códigos de error de EWS. Todos los demás mensajes se asignarán a `ERROR_FREE_BUSY_GENERATION_FAILED`.

Valor	Código de error de 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`

Concesión de acceso

Ejecute el siguiente comando de Lambda desde AWS Command Line Interface ()AWS CLI. Este comando añade una política de recursos a la función de Lambda que analiza el PAC. Esta función permite que el servicio de WorkMail disponibilidad de Amazon invoque su función 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
```

En el comando, añada los siguientes parámetros donde se indique:

- *LAMBDA_REGION*— Nombre de la región en la que se implementa el CAP Lambda. Por ejemplo, `us-east-1`.
- *CAP_FUNCTION_NAME*— Nombre de la función Lambda CAP.

> **Note**
>
> Puede ser el nombre, el alias o el ARN parcial o completo de la función de Lambda de CAP.

- *WM_REGION*— Nombre de la región en la que la WorkMail organización Amazon invoca la función Lambda.

> **Note**
>
> El uso con CAP está disponible solo en las siguientes regiones:
>
> - Este de EE. UU. (Norte de Virginia)
> - Oeste de EE. UU. (Oregón)
> - Europa (Irlanda)

- *WM_ACCOUNT_ID*— El ID de la cuenta de la organización.
- *ORGANIZATION_ID*— El ID de la organización que invoca el CAP Lambda. Por ejemplo, ID de org.: m-934ebb9eb57145d0a6cab566ca81a21f.

> **Note**
>
> *LAMBDA_REGION*y solo *WM_REGION* será diferente si se necesitan llamadas entre regiones. Si las llamadas entre regiones no son necesarias, serán la misma.

Ejemplo de Amazon WorkMail utilizando una función CAP Lambda

Para ver un ejemplo de cómo Amazon WorkMail utiliza una función de CAP Lambda para consultar un punto final de EWS, consulte este AWS ejemplo de aplicación en el repositorio Serverless Applications for Amazon. WorkMail GitHub

Configuración de los parámetros de disponibilidad en Microsoft Exchange

Para redirigir a Amazon todas las solicitudes de información de disponibilidad o ocupación del calendario para los usuarios habilitados WorkMail, configura un espacio de direcciones de disponibilidad en Microsoft Exchange.

Usa el siguiente PowerShell comando para crear el espacio de direcciones:

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

Cuando se te pida, introduce las credenciales de la cuenta de WorkMail servicio de Amazon. El nombre de usuario se debe introducir como **domain\username** (es decir, ***orgname*.awsapps.com\workmail_service_account_*username***. Aquí, ***orgname*** representa el nombre de la WorkMail organización Amazon. Para obtener más información, consulte Crear cuentas de servicio en Microsoft Exchange y Amazon WorkMail.

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

Para obtener más información, consulte Complementos AvailabilityAddressSpace de Microsoft Docs.

Habilite el enrutamiento de correo electrónico entre WorkMail los usuarios de Microsoft Exchange y Amazon

Con el enrutamiento de correo electrónico entre Microsoft Exchange Server y Amazon WorkMail, los usuarios pueden conservar sus direcciones de correo electrónico actuales después de migrar a Amazon WorkMail. El enrutamiento de correo electrónico le permite mantener Microsoft Exchange Server como servidor principal del Protocolo simple de transferencia de correo (SMTP) para el correo electrónico entrante de su organización.

Antes de utilizar el enrutamiento de correo electrónico, debe satisfacer los siguientes requisitos previos:

- Habilitar el modo de interoperabilidad para su organización. Para obtener más información, consulte Habilitación de la interoperabilidad.
- Asegúrate de ver tu dominio en la WorkMail consola de Amazon.

- Verificar que nuestro Microsoft Exchange Server pueda enviar correo electrónico a Internet. Es posible que necesite configurar un conector de envío. Para obtener más información sobre los conectores de envío, consulte Creación de un conector de envío en Exchange Server para enviar correo a Internet en la documentación de Microsoft.

Habilitar el direccionamiento de correo electrónico para un usuario

Le recomendamos que primero complete los siguientes pasos para usuarios de prueba antes de aplicar cualquier cambio a su organización.

1. Activa la cuenta de usuario que vas a migrar a Amazon WorkMail. Para obtener más información, consulte Habilitación de usuarios existentes.
2. En la WorkMail consola de Amazon, asegúrate de que haya al menos dos direcciones de correo electrónico asociadas al usuario habilitado.
   - <*workmailuser*@ *orgname* .awsapps.com> (se agrega automáticamente y se puede usar para pruebas sin Microsoft Exchange).
   - <*workmailuser*@ *yourdomain* .com> (se agrega automáticamente y es la dirección principal de Microsoft Exchange).

     Para obtener más información, consulte Modificación de direcciones de correo electrónico de los usuarios.
3. Asegúrese de migrar todos los datos del buzón de Microsoft Exchange al buzón de Amazon WorkMail. Para obtener más información, consulta Migración a Amazon WorkMail.
4. Una vez migrados todos los datos, deshabilite el buzón de correo del usuario en Microsoft Exchange. A continuación, cree un usuario de correo (o un usuario con correo habilitado) que tenga la dirección SMTP externa apuntando a Amazon. WorkMail Para ello, utilice los siguientes comandos en el intérprete de comandos de administración de Exchange:

> **Important**
>
> Los siguientes pasos borran el contenido del buzón de correo. Asegúrese de que sus datos se hayan migrado a Amazon WorkMail antes de intentar habilitar el enrutamiento del correo electrónico. Algunos clientes de correo no cambian sin problemas a Amazon WorkMail cuando ejecutas este comando. Para obtener más información, consulte Configuración del cliente de correo.

```
$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
```

En los comandos anteriores, *orgname* representa el nombre de tu WorkMail organización de Amazon. Para obtener más información, consulte Deshabilitar el buzón y Habilitar los usuarios de correo en Microsoft TechNet.

5. Envíe un correo electrónico de prueba al usuario (en el ejemplo anterior, **workmailuser@yourdomain.com**). Si el enrutamiento del correo electrónico se ha habilitado correctamente, el usuario debería poder iniciar sesión en su WorkMail buzón de Amazon y recibir el correo electrónico.

> **Note**
>
> Microsoft Exchange sigue siendo el servidor principal para los correos electrónicos entrantes siempre que usted quiera tener interoperabilidad entre los dos entornos. Para garantizar la interoperabilidad con Microsoft Exchange, los registros de DNS no deberían actualizarse para que apunten a Amazon WorkMail hasta más tarde.

Tareas posteriores a la configuración

Los pasos anteriores mueven el buzón de un usuario de Microsoft Exchange Server a Amazon WorkMail, manteniendo al usuario en Microsoft Exchange como contacto. Dado que el usuario migrado es ahora un usuario de correo externo, Microsoft Exchange Server impone restricciones adicionales. También puede haber requisitos de configuración adicionales para completar la migración.

- El usuario podría no ser capaz de enviar correos electrónicos a grupos de forma predeterminada. Para habilitar esta funcionalidad, debe añadir el usuario a una lista de remitentes seguros para todos los grupos. Para obtener más información, consulte Administración de entregas en Microsoft TechNet.
- Es posible que el usuario no pueda reservar recursos. Para habilitar esta funcionalidad, debe establecer el `ProcessExternalMeetingMessages` de todos los recursos a los que el usuario necesite acceder. Para obtener más información, consulte Set- CalendarProcessing on Microsoft TechNet.

Configuración del cliente de correo

Algunos clientes de correo no se cambian fácilmente a Amazon WorkMail. Estos clientes requieren que el usuario realice pasos de configuración adicionales. Diferentes clientes de correo exigen realizar diferentes acciones.

- Microsoft Outlook en Windows: requiere el reinicio de Outlook. Al iniciar, tiene que elegir entre seguir usando el buzón de correo anterior o usar un buzón de correo temporal. Elija la opción de buzón de correo temporal. A continuación, reconfigure el buzón de correo de Microsoft Exchange.
- Microsoft Outlook en macOS: cuando se reinicie Outlook, aparecerá el siguiente mensaje: Outlook se redirigió al servidor ***orgname*** .awsapps.com. ¿Desea que este servidor configure sus ajustes? Acepte la sugerencia.
- Mail en iOS: la aplicación de correo deja de recibir correos electrónicos y genera un error no se puede recibir correo. Vuelva a crear y configurar el buzón de correo de Microsoft Exchange.

Deshabilitación del modo de interoperabilidad y baja de su servidor de correo

Después de configurar los buzones de Microsoft Exchange para Amazon WorkMail, puede deshabilitar el modo de interoperabilidad. Si no ha migrado ningún usuario o registro, deshabilitar el modo de interoperabilidad no afecta a ninguna de sus configuraciones.

> **Warning**
>
> Antes de deshabilitar el modo de interoperabilidad, asegúrese de completar todos los pasos necesarios. No hacerlo podría dar lugar a correos electrónicos rebotados

o a comportamientos no deseados. Si no ha completado la migración, deshabilitar la interoperabilidad puede causar interrupciones en su organización. No podrá deshacer esta operación.

Para deshabilitar el soporte de modo de interoperabilidad

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, seleccione la organización para la que desea deshabilitar el modo de interoperabilidad.
3. En Configuración de la organización, elija Deshabilitar modo de interoperabilidad.
4. En el cuadro de diálogo Desactivar modo de interoperabilidad, introduzca el nombre de la organización y elija Desactivar modo de interoperabilidad.

Tras inhabilitar la compatibilidad con la interoperabilidad, los usuarios y grupos que no estén habilitados para Amazon WorkMail se eliminarán de la libreta de direcciones. Puedes seguir habilitando cualquier usuario o grupo que falte mediante la WorkMail consola de Amazon y se añadirán a la libreta de direcciones. Los recursos de Microsoft Exchange no se pueden habilitar y no aparecen en la libreta de direcciones hasta que se complete el paso siguiente.

- Crear recursos en Amazon WorkMail: puede crear recursos en Amazon WorkMail y, a continuación, configurar los delegados y las opciones de reserva para estos recursos. Para obtener más información, consulte Uso de recursos.
- Crear un registro AutoDiscover DNS: configure un registro AutoDiscover DNS para todos los dominios de correo de la organización. Esto permite a los usuarios conectarse a sus WorkMail buzones de Amazon desde sus clientes móviles y de Microsoft Outlook. Para obtener más información, consulte Uso AutoDiscover para configurar puntos de conexión.
- Cambia tu registro DNS MX a Amazon WorkMail: para enviar todos los correos electrónicos entrantes a Amazon WorkMail, debes cambiar tu registro DNS MX a Amazon WorkMail. Los cambios en los registros DNS pueden tardar hasta 72 horas en propagarse a todos los servidores DNS.

- Retirar tu servidor de correo: una vez que hayas verificado que todo el correo electrónico se envía directamente a Amazon WorkMail, puedes desmantelar tu servidor de correo si no tienes intención de usarlo en el futuro.

Solución de problemas

A continuación se detallan las soluciones a los errores de WorkMail interoperabilidad y migración más frecuentes de Amazon.

El URL del servicio web de Exchange (EWS) no es válido o es inaccesible: compruebe que tiene el URL de EWS correcto. Para obtener más información, consulte Configurar los ajustes de disponibilidad en Amazon WorkMail.

Fallo de conexión durante la validación de EWS: se trata de un error general y podría deberse a:

- Sin conexión a Internet en Microsoft Exchange.
- El firewall no está configurado para permitir acceso desde Internet. Asegúrese de que el puerto 443 (el puerto predeterminado para HTTPS) esté abierto.

Si ha confirmado la conexión a Internet y la configuración del cortafuegos, pero el error persiste, póngase en contacto con AWS Support.

Nombre de usuario y contraseña no válidos al configurar la interoperabilidad de Microsoft Exchange: se trata de un error general y podría deberse a:

- El nombre de usuario no tiene el formato esperado. Use el siguiente patrón:

```
DOMAIN\username
```

- El servidor de Microsoft Exchange no está configurado para la autenticación básica para EWS. Para obtener más información, consulte Directorios virtuales: Exchange 2013 en el blog Microsoft MVP Award Program.

El usuario recibe correos electrónicos con el archivo adjunto winmail.dat: esto puede ocurrir cuando se envía correo electrónico S/MIME cifrado de Exchange a Amazon WorkMail y se recibe en Outlook 2016 para Mac o en un cliente IMAP. La solución es ejecutar el siguiente comando en el intérprete de comandos de administración de Exchange.

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

Si ha confirmado los puntos anteriores pero el error persiste, contacte con AWS Support.

WorkMail Cuotas de Amazon

Amazon WorkMail puede ser utilizado tanto por clientes empresariales como por propietarios de pequeñas empresas. Si bien damos soporte a la mayoría de los casos de uso sin tener que configurar ningún cambio en las cuotas, también protegemos a nuestros usuarios e Internet frente al abuso del producto. Por tanto, algunos clientes podrían alcanzar las cuotas que hemos establecido. En esta sección se describen estas cuotas y cómo cambiarlas.

Algunos valores de cuota se pueden modificar y otros son cuotas fijas que no se pueden modificar. Para obtener más información acerca de cómo solicitar un aumento de cuotas, consulte Cuotas de servicio de AWS en Referencia general de Amazon Web Services.

Cuotas WorkMail de organización y usuarios de Amazon

Puedes añadir hasta 25 usuarios a tu WorkMail organización de Amazon para disfrutar de una prueba gratuita de 30 días. Una vez finalizado este período, se te cobrará por todos los usuarios activos, a menos que los elimines o cierres tu WorkMail cuenta de Amazon.

Todos los mensajes que se envían a otro usuario se tienen en cuenta al evaluar estas cuotas. Incluyen mensajes de correo electrónico, solicitudes de reuniones, respuestas de reuniones, solicitudes de tareas y mensajes que se reenvían o redirigen automáticamente como consecuencia de una regla.

> **Note**
>
> Al solicitar un aumento de cuota para una organización específica, debe incluir el nombre de la organización en su solicitud.

Recurso	Cuota predeterminada	Límite superior para solicitudes de cambio
WorkMail Organizaciones de Amazon por AWS cuenta	100	Se puede aumentar en función del tipo de directorio de una

Recurso	Cuota predeterminada	Límite superior para solicitudes de cambio
		organización. Puedes ver AWS Directory Service las cuotas y solicitar aumentos desde la AWS Directory Service consola. Para obtener más información, consulte Cuotas de servicios en la Referencia general de AWS.

Recurso	Cuota predeterminada	Límite superior para solicitudes de cambio
Usuarios por WorkMail organización de Amazon	1 000	Se puede aumentar en función del tipo de directorio de la organización, como se indica a continuación: • WorkMail Directorio Amazon: hasta 10 millones de usuarios • Simple AD o conector AD, grande: un máximo de 5000 usuarios* • Simple AD o conector AD, pequeño: un máximo de 500 usuarios* • Microsoft AD, hospedado por AWS Directory Service: hasta 10 millones de usuarios, según su configuración y configuración, *Si está utilizando Simple AD o conector AD, consulte AWS Directory Service para obtener información adicional.
Usuarios de la prueba gratuita	Un máximo de 25 usuarios los primeros 30 días	El periodo de prueba gratuito solo es aplicable para los primeros 25 usuarios de cualquier organización. Cualquier usuario adicional no está incluido en la oferta de prueba gratuita.

Recurso	Cuota predeterminada	Límite superior para solicitudes de cambio
Destinatarios dirigidos por AWS cuenta y día	100 000 destinatarios externos a la organización, sin cuota rígida para destinatarios internos de la organización	No hay límite superior. Sin embargo, Amazon WorkMail es un servicio de correo electrónico empresarial y no está destinado a ser utilizado para servicios de correo masivo. Para servicios masivos de correo electrónico, consulte Amazon SES o Amazon Pinpoint.
Destinatarios dirigidos por AWS cuenta y día utilizando cualquiera de los dominios de prueba	200 destinatarios, independientemente del destino	No obstante, el dominio de correo de prueba no se ha diseñado para uso a largo plazo. Le recomendamos que añada su propio dominio y lo utilice como dominio predeterminado.

Los límites de las cuotas se definen de acuerdo con el directorio subyacente.

WorkMail organización que establece cuotas

Recurso	Cuota predeterminada
Número de dominios por WorkMail organización de Amazon	1 000 Esta es una cuota fija que no se puede cambiar.
Número de patrones de remitente en reglas de flujo de correo electrónico por regla	250 Esta es una cuota fija que no se puede cambiar.

Recurso	Cuota predeterminada
Número de patrones de remitente en reglas de flujo de correo electrónico por organización	1 000 Esta es una cuota fija que no se puede cambiar.

Cuotas por usuario

Todos los mensajes que se envían a otro usuario se tienen en cuenta al evaluar estas cuotas. Incluyen mensajes de correo electrónico, solicitudes de reuniones, respuestas de reuniones, solicitudes de tareas y mensajes que se reenvían o redirigen automáticamente como consecuencia de una regla.

Recurso	Cuota predeterminada	Cuota superior para solicitudes de cambio
Tamaño máximo del buzón de correo	50 GB Esta es una cuota fija que no se puede cambiar.	No aplicable
Número máximo de alias por usuario	100 Esta es una cuota fija que no se puede cambiar.	No aplicable
Destinatarios contactados por usuario por día utilizando el dominio del cual es propietario	10 000 destinatarios externos a la organización, sin cuota rígida para destinatarios internos de la organización	No hay límite superior. Sin embargo, Amazon WorkMail es un servicio de correo electrónico empresarial y no está destinado a ser utilizado para servicios de correo masivo. Para servicios masivos de correo electrónico, consulte Amazon SES o Amazon Pinpoint.

Cuotas de mensajes

Todos los mensajes que se envían a otro usuario se tienen en cuenta al evaluar estas cuotas. Incluyen mensajes de correo electrónico, solicitudes de reuniones, respuestas de reuniones, solicitudes de tareas y mensajes que se reenvían o redirigen automáticamente como consecuencia de una regla.

Recurso	Cuota predeterminada
Tamaño máximo del mensaje entrante	29 MB de datos sin codificar. Los mensajes se reciben en formato MIME. El tamaño máximo del mensaje MIME entrante es de 40 MB. Esta es una cuota fija que no se puede cambiar.
Tamaño máximo del mensaje saliente	29 MB de datos sin codificar. Los mensajes se envían en formato MIME. El tamaño máximo del mensaje MIME saliente es de 40 MB. Esta es una cuota fija que no se puede cambiar.
Número máximo de destinatarios por mensaje	500 Esta es una cuota fija que no se puede cambiar.
Cantidad máxima de archivos adjuntos por mensaje	500 Esta es una cuota fija que no se puede cambiar.

Uso de organizaciones

En Amazon WorkMail, tu organización representa a los usuarios de tu empresa. En la WorkMail consola de Amazon, verás una lista de las organizaciones disponibles. Si no tienes ninguna disponible, debes crear una organización para poder utilizar Amazon WorkMail.

Temas

Creación de una organización

Para usar Amazon WorkMail, primero debes crear una organización. Una AWS cuenta puede tener varias WorkMail organizaciones de Amazon. Al crear una organización, también debe seleccionar un dominio para la organización y configurar el directorio de usuarios y los ajustes de cifrado.

Puedes crear un nuevo directorio de usuarios o integrar Amazon WorkMail con un directorio existente. Puedes usar Amazon WorkMail con un Microsoft Active Directory local, un Active Directory AWS administrado o un Simple AD. Al integrarlo con tu directorio local, puedes usar tus usuarios y grupos existentes en Amazon WorkMail y los usuarios pueden iniciar sesión con sus credenciales existentes. Si utiliza un directorio en las instalaciones, primero debe configurar un conector AD en AWS Directory Service. El AD Connector sincroniza los usuarios y grupos con la libreta de WorkMail direcciones de Amazon y realiza las solicitudes de autenticación de los usuarios. Para obtener más información, consulte Conector Active Directory en la Guía de administración de AWS Directory Service .

También tienes la opción de seleccionar una AWS KMS key que Amazon WorkMail utilice para cifrar el contenido del buzón. Puedes seleccionar la clave maestra AWS gestionada predeterminada para Amazon WorkMail o usar una clave de KMS existente en AWS Key Management Service (AWS

KMS). Para obtener información sobre la creación de una nueva clave de KMS, consulte Creación de claves en la Guía para desarrolladores de AWS Key Management Service . Si ha iniciado sesión como usuario AWS Identity and Access Management (IAM), conviértase en administrador de claves de la clave de KMS. Para obtener más información, consulte Habilitación y deshabilitación de claves en la Guía para desarrolladores de AWS Key Management Service .

Consideraciones

Recuerda lo siguiente al crear una WorkMail organización de Amazon:

- Amazon WorkMail no admite actualmente los servicios gestionados de Microsoft Active Directory que compartes con varias cuentas.
- Si dispone de Active Directory con Microsoft Exchange y un conector AD en las instalaciones, le recomendamos que configure los ajustes de interoperabilidad para su organización. Esto le permite minimizar las molestias para sus usuarios al migrar los buzones a Amazon WorkMail o utilizar Amazon WorkMail para un subconjunto de sus buzones corporativos. Para obtener más información, consulte Interoperabilidad entre Amazon WorkMail y Microsoft Exchange.
- Si seleccionas la opción Dominio de prueba gratuito, puedes empezar a utilizar tu WorkMail organización de Amazon con el dominio de prueba proporcionado. El dominio de prueba usa este formato: *example* .awsapps.com. Puedes usar el dominio de correo de prueba con Amazon WorkMail y otros AWS servicios compatibles siempre y cuando mantengas usuarios habilitados en tu WorkMail organización de Amazon. Sin embargo, no puede utilizar el dominio de prueba para otros fines. El dominio de prueba podría estar disponible para que otros clientes lo registren y lo utilicen si tu WorkMail organización de Amazon no tiene al menos un usuario habilitado.
- Amazon WorkMail no admite directorios multirregionales.

Temas

- Creación de una organización
- Visualización de detalles de una organización
- Integrar un WorkSpaces directorio
- Estados de la organización y sus descripciones

Creación de una organización

Crea una nueva organización en la WorkMail consola de Amazon.

Para crear una organización de

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.

2. En la barra de navegación, seleccione Organización.

   Aparece la página Organizaciones, en la que se muestran sus organizaciones, si las tiene.

3. Seleccione Crear organización.

4. En Dominio de correo electrónico, seleccione el dominio que desee utilizar para las direcciones de correo electrónico de su organización:

   - Dominio de Route 53 existente: seleccione un dominio existente que administre con una zona alojada de Amazon Route 53 (Route 53).
   - Nuevo dominio de Route 53: registra un nuevo nombre de dominio de Route 53 para usarlo con Amazon WorkMail.
   - Dominio externo: introduzca un dominio existente que administre con un proveedor de sistema de nombres de dominio (DNS) externo.
   - Dominio de prueba gratuito: utiliza un dominio de prueba gratuito proporcionado por Amazon WorkMail. Puedes explorar Amazon WorkMail con un dominio de prueba y, posteriormente, añadir un dominio a tu organización.

5. (Opcional) Si su dominio se administra a través de Amazon Route 53, en Zona alojada de Route 53, seleccione su dominio de Route 53.

6. En Alias, introduzca un alias único para su organización.

7. Elija Configuración avanzada y en Directorio de usuarios, elija una de las siguientes opciones:

   - Crear un nuevo WorkMail directorio de Amazon: crea un nuevo directorio para añadir y gestionar tus usuarios.
   - Utilizar directorio existente: utiliza un directorio existente para administrar sus usuarios, como Microsoft Active Directory, AWS Managed Active Directory o Simple AD en las instalaciones.

8. En Cifrado, seleccione una de las siguientes opciones:

- Usa una clave WorkMail gestionada por Amazon: crea una nueva clave de cifrado en tu cuenta.
- Utilizar una clave de KMS existente: utiliza una clave de KMS existente que ya ha creado en AWS KMS.

9. Seleccione Crear organización.

Si utiliza un dominio externo, verifíquelo añadiendo los registros de texto (TXT) y de intercambiador de correo (MX) apropiados a su servicio DNS. Los registros TXT le permiten introducir notas sobre el servicio DNS. Los registros MX especifican el servidor de correo entrante.

Asegúrese de establecer su dominio como predeterminado para su organización. Para obtener más información, consulte Verificación de dominios y Elección del dominio predeterminado.

Cuando su organización esté Activa, podrá añadirle usuarios y configurar sus clientes de correo electrónico. Para obtener más información, consulta Agregar un usuario Configuración de clientes de correo electrónico para Amazon WorkMail.

Visualización de detalles de una organización

Cada una de tus WorkMail organizaciones de Amazon puede mostrar una página de detalles de la organización. La página muestra información sobre su organización, incluida la IDs que puede utilizar con la AWS Command Line Interface. Los mensajes de la página también pueden mostrarle los pasos necesarios para finalizar la configuración de una organización, como un dominio no verificado o la falta de usuarios. Los mensajes también le indican el primer paso que debe seguir para configurar un determinado cliente de correo electrónico.

Para ver los detalles de la organización

1. En la barra de navegación, seleccione Organización.

   Aparece la página Organizaciones, en la que se muestran sus organizaciones.

2. Elija la organización que desee ver.

Integrar un WorkSpaces directorio

Para usar Amazon WorkMail con WorkSpaces, crea un directorio compatible siguiendo estos pasos.

Para añadir un WorkSpaces directorio compatible

1. Cree un directorio compatible utilizando WorkSpaces. Para obtener WorkSpaces instrucciones, consulta Cómo empezar con Amazon WorkSpaces Quick Setup en la Guía de WorkSpaces administración de Amazon.
2. En la WorkMail consola de Amazon, crea tu WorkMail organización de Amazon y elige usar tu directorio existente para ella. Para obtener más información, consulte Creación de una organización.

Estados de la organización y sus descripciones

Después de crear una organización, puede tener uno de los siguientes estados.

Estado	Descripción
Activo	Su organización está en buen estado y lista para su uso.
Creando	Se ejecuta un flujo de trabajo para crear su organización.
Con error	No se pudo crear su organización.
Deteriorado	Su organización no funciona correctamente o se ha detectado un problema.
Inactivo	Su organización está inactiva.
Solicitada	Su solicitud de creación de organización está en la cola y a la espera de creación.
Validación	Se está comprobando toda la configuración de la organización.

Eliminar una organización

Si ya no quieres usar Amazon WorkMail para el correo electrónico de tu organización, puedes eliminar tu organización de Amazon WorkMail.

> **Note**
>
> Esta operación no se puede deshacer. Tras eliminar una organización, ya no podrá recuperar los datos de su buzón de correo.

Eliminación de una organización

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En la pantalla Organizaciones, en la lista de organizaciones, seleccione la organización que desee eliminar y elija Eliminar.
3. En Eliminar organización, elija si desea eliminar o conservar el directorio de usuarios existente y, a continuación, introduzca el nombre de la organización.
4. Elija Eliminar organización.

> **Note**
>
> Si no proporcionaste tu propio directorio para Amazon WorkMail, crearemos uno para ti. Si conservas este directorio existente al eliminar la organización, se te cobrará por él, a menos que Amazon WorkMail, WorkDocs, o lo esté utilizando WorkSpaces. Para obtener información sobre los precios, consulte este artículo acerca de los precios de otros tipos de directorios.
> Para eliminar el directorio, no puede tener ninguna otra AWS aplicación habilitada. Para obtener más información, consulte Eliminación de un directorio de Simple AD o Eliminación de un directorio de conector AD en la Guía de administración de AWS Directory Service .

Es posible que reciba un mensaje de error de conjunto de reglas no válido de Amazon Simple Email Service (Amazon SES) al intentar eliminar una organización. Si recibe este error, edite la regla de Amazon SES en la consola de Amazon SES y elimine el conjunto de reglas no válido. La regla que edites debe incluir tu ID de WorkMail organización de Amazon en el nombre de la regla. Para

obtener más información sobre la edición de reglas de Amazon SES, consulte Creación de reglas de recepción en la Guía para desarrolladores de Amazon Simple Email Service.

Si necesita averiguar qué conjunto de reglas no es válido, primero guarde la regla. Aparece un mensaje de error para el conjunto de reglas.

Buscar una dirección de correo electrónico

Puedes averiguar si una dirección de correo electrónico se utiliza en tu organización por usuario, recurso o grupo.

Para buscar una dirección de correo electrónico

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de una organización.
3. En la página de la organización, selecciona Buscar dirección de correo electrónico.
4. Elija Buscar.

Uso de los ajustes de la organización

En las siguientes secciones se explica cómo utilizar la configuración disponible para WorkMail las organizaciones de Amazon. La configuración que elija se aplicará a toda la organización.

Temas

- Habilitación de la migración de buzones de correo
- Habilitación del registro histórico
- Habilitación de la interoperabilidad
- Habilitación de puertas de enlace SMTP
- Administración de flujos de correo electrónico

- Aplicación de políticas de DMARC en el correo electrónico entrante

Habilitación de la migración de buzones de correo

La migración de buzones se habilita cuando se quieren transferir buzones desde una fuente, como Microsoft Exchange o G Suite Basic, a Amazon WorkMail. Habilite la migración como parte de un proceso de migración más amplio. Para obtener más información, incluyendo los pasos a seguir, consulte Migración a Amazon WorkMail en la sección Introducción de esta guía.

Habilitación del registro histórico

Habilite el registro histórico para registrar sus comunicaciones por correo electrónico. Al utilizar el registro histórico, suele utilizar herramientas integradas de archivado y eDiscovery de terceros. El registro histórico le ayuda a garantizar el cumplimiento de la normativa sobre almacenamiento de datos, protección de la privacidad y protección de la información.

Para obtener más información, incluyendo los pasos a seguir, consulte Cómo usar el registro diario del correo electrónico con Amazon WorkMail en la sección Introducción de esta guía.

Habilitación de la interoperabilidad

La interoperabilidad le permite migrar desde Microsoft Exchange y usar Amazon WorkMail como un subconjunto de sus buzones corporativos. Para obtener más información, incluyendo los pasos a seguir, consulte Configurar los ajustes de disponibilidad en Amazon WorkMail en la sección Introducción de esta guía.

Habilitación de puertas de enlace SMTP

Habilite las puertas de enlace del Protocolo simple de transferencia de correo (SMTP) para utilizarlas con las reglas de flujo de correo electrónico saliente. Las reglas de flujo de correo saliente te permiten enrutar los mensajes de correo electrónico enviados desde tu WorkMail organización de Amazon a través de una puerta de enlace SMTP. Para obtener más información, consulte Acciones de las reglas de correo electrónico saliente.

> **Note**
>
> Las puertas de enlace SMTP configuradas para las reglas de flujo de correo electrónico saliente deben ser compatibles con Seguridad de la capa de transporte (TLS) v1.2 utilizando

certificados de las principales autoridades de certificación. Solo se admite la autenticación básica.

Para configurar una gateway SMTP

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de una organización.
3. En el panel de navegación, elija Configuración de la organización.

   Aparece la página Configuración de la organización, que muestra un conjunto de pestañas.
4. Elija la pestaña Puertas de enlace SMTP y, a continuación, Crear puerta de enlace.
5. Introduzca lo siguiente:

   - Nombre de la puerta de enlace: introduzca un nombre único.
   - Dirección de la puerta de enlace: introduzca el nombre de host o la dirección IP de la puerta de enlace.
   - Número de puerto: introduzca el número de puerto de la puerta de enlace.
   - Nombre de usuario: introduzca un nombre de usuario.
   - Contraseña: introduzca una contraseña segura.
6. Seleccione Crear.

   La gateway SMTP está disponible para su uso con reglas de flujo de correo electrónico saliente.

Al configurar una puerta de enlace SMTP para utilizarla con una regla de flujo de correo electrónico saliente, los mensajes salientes intentan hacer coincidir la regla con una puerta de enlace SMTP. Los mensajes que coincidan con la regla se enrutan a la puerta de enlace SMTP correspondiente, que se encarga del resto de la entrega del correo electrónico.

Si Amazon WorkMail no puede acceder a la puerta de enlace SMTP, el sistema devuelve el mensaje de correo electrónico al remitente. Si esto ocurre, siga los pasos anteriores para corregir la configuración de la puerta de enlace.

Administración de flujos de correo electrónico

Como ayuda para administrar el correo electrónico, puede configurar Reglas de flujo de correo electrónico. Las reglas de flujo de correo electrónico pueden realizar una o varias acciones sobre los mensajes de correo electrónico en función de sus direcciones o dominios. Puede utilizar reglas de flujo de correo electrónico en las direcciones de correo electrónico o dominios de los remitentes y destinatarios.

Al crear una regla de flujo de correo electrónico, se especifica una acción de regla que se aplica a un correo electrónico al coincidir un patrón de regla especificado.

Temas

- Acciones de las reglas de correo electrónico entrante
- Acciones de las reglas de correo electrónico saliente
- Patrones de remitentes y destinatarios
- Creación de reglas de flujo de correo electrónico
- Edición de reglas de flujo de correo electrónico
- Configuración AWS Lambda para Amazon WorkMail
- Administrar el acceso a la API de Amazon WorkMail Message Flow
- Comprobación de una regla de flujo de correo electrónico
- Eliminación de una regla de flujo de correo electrónico

Acciones de las reglas de correo electrónico entrante

Las reglas de flujo de correo electrónico entrante evitan que el correo electrónico de remitentes no deseados llegue a los buzones de correo de sus usuarios. Las reglas de flujo de correo entrante, también denominadas acciones de reglas, se aplican automáticamente a todos los mensajes de correo electrónico enviados a cualquier persona de tu WorkMail organización de Amazon. Esto difiere de las reglas de correo electrónico para buzones individuales.

> **Note**
>
> Si lo desea, puede usar reglas con una AWS Lambda función para procesar el correo entrante antes de que se entregue a los buzones de sus usuarios. Para obtener más información sobre el uso de Lambda con Amazon WorkMail, consulte. Configuración AWS Lambda para Amazon WorkMail Para obtener más información acerca de Lambda, consulte la Guía para desarrolladores de AWS Lambda .

Las reglas de flujo de correo entrante, también denominadas acciones de reglas, se aplican automáticamente a todos los mensajes de correo electrónico enviados a cualquier persona de la WorkMail organización de Amazon. Esto difiere de las reglas de correo electrónico para buzones individuales.

Las siguientes acciones de regla definen cómo se trata el correo electrónico entrante. Para cada regla, se especifican patrones de remitente y destinatario junto con una de las siguientes acciones.

Acción	Descripción
Eliminar correo electrónico	Se ignora el mensaje de correo electrónico. No se entrega y no se notifica al remitente que la entrega no se ha producido.
Enviar respuesta de rebote	El mensaje de correo electrónico no se entrega y se notifica al remitente de la entrega fallida mediante un mensaje de rebote.
Deliver to junk folder	El mensaje de correo electrónico se entrega a las carpetas de correo no deseado o basura de los usuarios, incluso si el sistema de detección de spam de Amazon no lo identificó originalm ente como WorkMail correo no deseado.
Predeterminado/a	El mensaje de correo electrónico se entrega una vez comprobado por el sistema de detección de WorkMail spam de Amazon. El correo electrónico de spam se entrega a la carpeta de correo no deseado. Todos los

Acción	Descripción
	demás mensajes de correo electrónico se entregan en la bandeja de entrada. Otras reglas de flujo de correo electrónico con un patrón de remitente menos específico se omiten. Para añadir excepciones a reglas de flujo de correo electrónico basadas en dominios, configure la acción predeterminada con un patrón de remitente más específic o. Para obtener más información, consulte Patrones de remitentes y destinatarios.
Never deliver to junk folder (No entregar nunca en carpeta de correo no deseado)	El mensaje de correo electrónico siempre se entrega a las bandejas de entrada de los usuarios, incluso si el sistema de detección de spam de Amazon lo identifica como WorkMail spam. **Important** Si no utiliza el sistema de detección de spam predeterminado, podría exponer a sus usuarios a contenido de alto riesgo de las direcciones que especifiq ue.
¡Ejecuta AWS Lambda	Transfiere el mensaje de correo electrónico a una función de Lambda para su procesamiento antes de la entrega o durante la misma a las bandejas de entrada de los usuarios.

Note

El correo entrante se envía primero a Amazon SES y, después, a Amazon WorkMail. Si Amazon SES bloquea un mensaje de correo electrónico entrante, no se aplicarán las

acciones de reglas. Por ejemplo, Amazon SES bloquea un mensaje de correo electrónico al detectar un virus conocido o debido a reglas explícitas de filtrado de IP. La especificación de una acción de regla como, por ejemplo, Default (Predeterminada), Deliver to junk folder (Entregar a carpeta de correo no deseado) o Never deliver to junk folder (No entregar nunca a la carpeta de correo no deseado), no tiene ningún efecto.

Acciones de las reglas de correo electrónico saliente

Las reglas de flujo de correo electrónico saliente se utilizan para dirigir mensajes de correo electrónico a través de puertas de enlace SMTP o para bloquear el envío de mensajes de correo electrónico a destinatarios específicos. Para obtener más información sobre las puertas de enlace SMTP, consulte Habilitación de puertas de enlace SMTP.

También puede utilizar reglas de flujo de correo electrónico saliente para pasar el mensaje de correo electrónico a una función de AWS Lambda para su procesamiento una vez enviado el correo electrónico. Para obtener más información acerca de Lambda, consulte la Guía para desarrolladores de AWS Lambda .

Las siguientes acciones de regla definen cómo se trata el correo electrónico saliente. Para cada regla, se especifican patrones de remitente y destinatario junto con una de las siguientes acciones.

Acción	Descripción
Predeterminado	El mensaje de correo electrónico se envía a través del flujo normal.
Eliminar correo electrónico	El mensaje de correo electrónico se descarta. No se envía y el remitente no recibe una notificación.
Enviar respuesta de rebote	El mensaje de correo electrónico no se envía y se notifica al remitente con un mensaje de que el administrador ha bloqueado el mensaje de correo electrónico.
Route to SMTP gateway (Enviar a gateway SMTP)	El mensaje de correo electrónico se envía a través de una puerta de enlace SMTP configurada.

Acción	Descripción
Ejecución de Lambda	Transmite el mensaje de correo electrónico a una función de Lambda para su procesamiento antes del envío del mensaje de correo electrónico o durante el mismo.

Patrones de remitentes y destinatarios

Se puede aplicar una regla de flujo de correo electrónico a una dirección de correo específica o a todas las direcciones de correo electrónico bajo un dominio específico o un conjunto de dominios. Los patrones de remitente se definen para determinar las direcciones de correo a las que se aplica una regla.

Tanto los patrones de remitente como de destinatario adoptan una de las formas siguientes:

- Una dirección de correo electrónico coincide con una dirección de correo electrónico única; por ejemplo:

```
mailbox@example.com
```

- Un nombre de dominio coincide con todas las direcciones de correo electrónico bajo ese dominio; como por ejemplo:

```
example.com
```

- Un dominio comodín coincide con todas las direcciones de correo electrónico bajo ese dominio y todos sus subdominios. El comodín solo aparece delante de un dominio; por ejemplo:

```
*.example.com
```

- Una estrella coincide con todas las direcciones de correo electrónico bajo cualquier dominio.

```
*
```

> **Note**
>
> No se puede usar el símbolo + dentro de los patrones del remitente o destinatario.

Se pueden especificar varios patrones para una regla. Para obtener más información, consulte Acciones de las reglas de correo electrónico entrante y Acciones de las reglas de correo electrónico saliente.

Las reglas de flujo de correo electrónico entrante se aplican si el encabezado de `Sender` o `From` de un mensaje de correo electrónico entrante coincide con algún patrón. Si está presente, se empareja la dirección `Sender` en primer lugar. La dirección `From` se empareja si no hay encabezamiento `Sender` o si el encabezamiento `Sender` no coincide con ninguna regla. Si hay varios destinatarios para el mensaje de correo electrónico que coincidan con diferentes reglas, cada regla se aplica para los destinatarios coincidentes.

Las reglas de flujo de correo electrónico saliente se aplican si el destinatario y el encabezado de `Sender` o `From` de un mensaje de correo electrónico saliente coinciden con algún patrón. Si hay varios destinatarios para el mensaje de correo electrónico que coincidan con diferentes reglas, cada regla se aplica para los destinatarios coincidentes.

Si hay varias reglas coincidentes, se aplica la acción de la regla más específica. Un ejemplo es cuando una regla para una dirección de correo electrónico específica tiene prioridad sobre una regla para un dominio entero. Si varias reglas tienen el mismo nivel de especificidad, se aplica la acción más restrictiva. Un ejemplo es cuando una acción Drop (Eliminar) tiene prioridad sobre una acción Bounce (Rebote). El orden de preferencia para las acciones es el mismo que el orden en el que se enumeran en Acciones de las reglas de correo electrónico entrante y Acciones de las reglas de correo electrónico saliente.

> **Note**
>
> Tenga cuidado al crear reglas con patrones de remitente solapados con acciones Drop o Bounce. Un orden de precedencia inesperado podría hacer que muchos mensajes de correo electrónico entrantes no se entreguen.

Creación de reglas de flujo de correo electrónico

Las reglas de flujo de correo electrónico aplican acciones de regla a los mensajes de correo electrónico entrantes y salientes. Las acciones se aplican cuando los mensajes coinciden con un patrón especificado. Las nuevas reglas de flujo de correo electrónico entran en vigor de inmediato.

Para crear reglas de flujo de correo electrónico

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de una organización.
3. En el panel de navegación, elija Configuración de la organización.

   Aparece la página Configuración de la organización, que muestra un conjunto de pestañas. Desde esta página, puede crear reglas de entrada o de salida. Los siguientes pasos explican cómo crear ambos tipos.

   Creación de reglas de entrada

   1. Elija la pestaña Reglas de entrada y luego Crear.
   2. En el cuadro Nombre de la regla, introduzca un nombre único.
   3. En Acción, abra la lista y seleccione una acción. Cada elemento de la lista contiene una descripción y algunos proporcionan enlaces Más información.

      > **Note**
      >
      > Si elige la acción Ejecutar Lambda, aparecen controles adicionales: Para obtener información sobre el uso de esos controles, consulte la sección siguiente, Configuración AWS Lambda para Amazon WorkMail.

   4. En Dominios o direcciones de remitente, introduzca los dominios o direcciones de remitente a los que desea que se aplique la regla.

5. En Dominios o direcciones de destino, introduzca cualquier combinación de dominios y direcciones de correo electrónico de destino.
6. Seleccione Crear.

Para crear reglas de salida

1. Elija la pestaña Reglas de salida y luego Crear.
2. En el cuadro Nombre de la regla, introduzca un nombre único.
3. En Acción, abra la lista y seleccione una acción. Cada elemento de la lista contiene una descripción y algunos proporcionan enlaces Más información.

> **Note**
>
> Si selecciona la acción Ejecutar Lambda, aparecen controles adicionales. Para obtener información sobre el uso de esos controles, consulte la sección siguiente, Configuración AWS Lambda para Amazon WorkMail.

4. En Dominios o direcciones de remitente, introduzca cualquier combinación válida de dominios y direcciones de correo electrónico de remitente.
5. En Dominios o direcciones de destino, introduzca cualquier combinación válida de dominios y direcciones de correo electrónico de destino.
6. Seleccione Crear.

Puede probar la regla de flujo de correo electrónico nueva que ha creado. Para obtener más información, consulte Comprobación de una regla de flujo de correo electrónico.

Edición de reglas de flujo de correo electrónico

Edite las reglas de flujo de correo electrónico siempre que necesite cambiar una o varias acciones de regla para los mensajes de correo electrónico. Los pasos de esta sección se aplican a los mensajes de correo electrónico entrantes y salientes.

Edición de las reglas de flujo de correo electrónico

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de una organización.
3. En el panel de navegación, elija Configuración de la organización.

   Aparece la página Configuración de la organización, que muestra un conjunto de pestañas.
4. Elija las pestañas Reglas de entrada o Reglas de salida.
5. Elija el botón de opción situado junto a la regla que desee modificar y, a continuación, elija Editar.
6. Cambie las acciones de la regla según sea necesario y, a continuación, elija Guardar.

Configuración AWS Lambda para Amazon WorkMail

Utilice la acción Ejecutar Lambda en las reglas de flujo de correo entrante y saliente para pasar los mensajes de correo electrónico que cumplan las reglas a una AWS Lambda función para su procesamiento.

Elija una de las siguientes configuraciones para una acción de Ejecutar Lambda en Amazon. WorkMail

Configuración asincrónica de Ejecutar Lambda

Los mensajes de correo electrónico que coinciden con la regla de flujo se transfieren a una función de Lambda para su procesamiento antes de su envío o entrega. Utilice esta configuración para modificar el contenido del correo electrónico. También puede controlar el flujo de correo electrónico entrante o saliente para diferentes casos de uso. Por ejemplo, una regla transferida a una función de Lambda puede bloquear la entrega de mensajes de correo electrónico confidenciales, eliminar archivos adjuntos o añadir cláusulas de exención de responsabilidad.

Configuración sincrónica de Ejecutar Lambda

Los mensajes de correo electrónico que coinciden con la regla de flujo se transfieren a una función de Lambda para su procesamiento mientras se envían o entregan. Esta configuración no afecta a la entrega de correo electrónico y se utiliza para tareas como recopilar métricas de mensajes de correo electrónico entrantes o salientes.

Tanto si elige una configuración sincrónica como asincrónica, el objeto de evento transferido a su función de Lambda contiene metadatos para el evento de correo electrónico entrante o saliente. También puede usar el ID del mensaje en los metadatos para acceder al contenido completo del mensaje de correo electrónico. Para obtener más información, consulte Recuperar el contenido de los mensajes con AWS Lambda. Para obtener más información acerca de los eventos de correo electrónico, consulte Datos de eventos de Lambda.

Para obtener más información acerca de las reglas de flujo de correo electrónico entrante y saliente, consulte Administración de flujos de correo electrónico. Para obtener más información acerca de Lambda, consulte la Guía para desarrolladores de AWS Lambda .

> **Note**
>
> Actualmente, las reglas de flujo de correo electrónico de Lambda solo hacen referencia a las funciones de Lambda de la misma región de AWS y de Cuenta de AWS la organización de Amazon WorkMail que se está configurando.

Primeros pasos con AWS Lambda Amazon WorkMail

Para empezar a utilizarla AWS Lambda con Amazon WorkMail, te recomendamos implementar la función WorkMail Hello World Lambda desde tu AWS Serverless Application Repository cuenta. La función cuenta con todos los recursos necesarios y los permisos configurados para usted. Para ver más ejemplos, consulta el amazon-workmail-lambda-templatesrepositorio en GitHub.

Si decide crear su propia función Lambda, debe configurar los permisos mediante AWS Command Line Interface ()AWS CLI. En el siguiente comando de ejemplo, haga lo siguiente:

- Sustituya `MY_FUNCTION_NAME` por el nombre de su función de Lambda.
- `REGION`Sustitúyala por tu región WorkMail de Amazon AWS. Las WorkMail regiones de Amazon disponibles incluyen `us-east-1` (EE.UU. Este (Norte de Virginia)), `us-west-2` (EE.UU. Oeste (Oregón)) y `eu-west-1` (Europa (Irlanda)).
- Sustituya `AWS_ACCOUNT_ID` por su ID de Cuenta de AWS de 12 dígitos.
- `WORKMAIL_ORGANIZATION_ID`Sustitúyelo por tu identificador de WorkMail organización de Amazon. Puede encontrarlo en la ficha de su organización en la página Organizaciones.

```
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
```

Para obtener más información sobre el uso de AWS CLI, consulta la Guía del AWS Command Line Interface usuario.

Configuración de reglas de Ejecutar Lambda sincrónicas

Para configurar una regla de Ejecutar Lambda sincrónica, cree una regla de flujo de correo electrónico con la acción Ejecutar Lambda y seleccione la casilla Ejecutar en sincronía. Para obtener más información acerca de la creación de reglas de flujo de correo, consulte Creación de reglas de flujo de correo electrónico.

Para terminar de crear la regla sincrónica, añada el Nombre de recurso de Amazon (ARN) de Lambda y configure las siguientes opciones.

Acción alternativa

La acción que Amazon WorkMail aplica si la función Lambda no se ejecuta. Esta acción también se aplica a los destinatarios que se omitan en la respuesta de Lambda si no se establece el indicador allRecipients. La Acción alternativa no puede ser otra acción de Lambda.

Tiempo de espera de regla (en minutos)

El período de tiempo durante el que se vuelve a intentar la función Lambda si Amazon WorkMail no la invoca. La Acción alternativa se aplica al final de este período de tiempo.

> **Note**
>
> Las reglas de Ejecutar Lambda sincrónicas solo admiten la condición de destino *****.

Datos de eventos de Lambda

La función de Lambda se activa a través de los siguientes datos de eventos. La presentación de los datos varía en función del lenguaje de programación utilizado para la función de 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
}
```

El JSON del evento incluye los siguientes datos.

summaryVersion

El número de versión de `LambdaEventData`. Solo se actualiza al realizar un cambio incompatible con versiones anteriores en `LambdaEventData`.

sobre

El sobre del mensaje de correo electrónico, que incluye los siguientes: campos.

mailFrom

La dirección De, que suele ser la dirección de correo electrónico del usuario que envió el mensaje. Si el usuario envió el mensaje de correo electrónico como otro usuario o en nombre de otro usuario, el campo mailFrom devuelve la dirección de correo electrónico del usuario en cuyo nombre se ha enviado el correo electrónico, no la dirección de correo electrónico del remitente real.

recipients

Una lista de todas las direcciones de correo electrónico de los destinatarios. Amazon WorkMail no distingue entre To, CC o BCC.

> **Note**
>
> En el caso de las reglas de flujo de correo entrante, esta lista incluye los destinatarios de todos los dominios de la WorkMail organización de Amazon en la que has creado la regla. La función de Lambda se invoca por separado para cada conversación SMTP del remitente y el campo de destinatarios enumera los destinatarios de esa conversación SMTP. Los destinatarios con dominios externos no se incluyen.

remitente

La dirección de correo electrónico del usuario que envió el mensaje de correo electrónico en nombre de otro usuario. Este campo se establece únicamente cuando un mensaje de correo electrónico se envía en nombre de otro usuario.

subject

La línea de asunto del correo electrónico. Se trunca cuando supera el límite de 256 caracteres.

messageId

Un identificador único que se utiliza para acceder a todo el contenido del mensaje de correo electrónico cuando se utiliza el SDK de Amazon WorkMail Message Flow.

invocationId

El ID de una invocación de Lambda única. Este identificador permanece igual cuando se llama a una función Lambda más de una vez para la misma función. LambdaEventData Utilícelo para detectar reintentos y evitar duplicaciones.

flowDirection

Indica la dirección del flujo de correo electrónico, bien ENTRANTE o SALIENTE.

truncated

Se aplica al tamaño de carga, no a la longitud de la línea de asunto. Si es `true`, el tamaño de la carga supera el límite de 128 KB, por lo que la lista de destinatarios se trunca para no superar el límite.

Esquema de respuesta de Ejecutar Lambda sincrónica

Cuando una regla de flujo de correo electrónico con una acción sincrónica Ejecutar Lambda coincide con un mensaje de correo entrante o saliente, Amazon WorkMail llama a la función Lambda configurada y espera la respuesta antes de realizar una acción en el mensaje de correo electrónico. La función de Lambda devuelve una respuesta conforme a un esquema predefinido que enumera las acciones, los tipos de acción, los parámetros aplicables y los destinatarios a los que se aplica la acción.

En el siguiente ejemplo se muestra una respuesta de Ejecutar Lambda sincrónica. Las respuestas varían en función del lenguaje de programación utilizado para la función de Lambda.

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

El JSON de respuesta incluye los siguientes datos.

acción

La acción que se debe realizar para los destinatarios.

type

El tipo de acción. Los tipos de acción no se devuelven para las acciones Ejecutar Lambda asincrónicas.

Los tipos de acción de reglas entrantes incluyen BOUNCE, DROP, DEFAULT, BYPASS_SPAM_CHECK y MOVE_TO_JUNK. Para obtener más información, consulte Acciones de las reglas de correo electrónico entrante.

Los tipos de acción de regla de salida incluyen BOUNCE, DROP y DEFAULT. Para obtener más información, consulte Acciones de las reglas de correo electrónico saliente.

parameters

Parámetros de acción adicionales. Se admite para el tipo de acción BOUNCE como un objeto JSON con la clave bounceMessage y la cadenade valor. Este mensaje de rebote se utiliza para crear el mensaje de correo electrónico de rebote.

recipients

Lista de direcciones de correo electrónico en las que se debe realizar la acción. Puede agregar nuevos destinatarios a la respuesta aunque no se hayan incluido en la lista de destinatarios original. Este campo no es obligatorio si allRecipients es true para una acción.

> **Note**
>
> Cuando se llama a una acción de Lambda para el correo electrónico entrante, solo puede añadir nuevos destinatarios que sean de su organización. Los nuevos destinatarios se agregan a la respuesta como CCO.

allRecipients

Cuando es verdadero, aplica la acción a todos los destinatarios que no estén sujetos a otra acción específica en la respuesta de Lambda.

Límites de la acción Ejecutar Lambda sincrónica

Los siguientes límites se aplican cuando Amazon WorkMail invoca funciones de Lambda para acciones sincrónicas de Run Lambda:

- Las funciones de Lambda deben responder en un plazo de 15 segundos o se tratarán como invocaciones fallidas.

  > **Note**
  >
  > El sistema reintenta la invocación tras el intervalo Tiempo de espera de regla que usted especifique.

- Se permiten respuestas de funciones de Lambda de hasta 256 KB.
- Se permiten hasta 10 acciones únicas en la respuesta. Las acciones mayores de 10 están sujetas a la Acción de reserva configurada.

- Se permiten hasta 500 destinatarios para las funciones de Lambda salientes.
- El valor máximo para el Tiempo de espera de regla es de 240 minutos. Si se configura el valor mínimo de 0, no habrá reintentos antes de que Amazon WorkMail aplique la acción alternativa.

Fallos de la acción Ejecutar Lambda sincrónica

Si Amazon no WorkMail puede invocar la función Lambda debido a un error, una respuesta no válida o un tiempo de espera de Lambda, WorkMail Amazon vuelve a intentar la invocación con un retraso exponencial que reduce la velocidad de procesamiento hasta que se complete el período de tiempo de espera de la regla. A continuación, se aplica la Acción de reserva a todos los destinatarios del mensaje de correo electrónico. Para obtener más información, consulte Configuración de reglas de Ejecutar Lambda sincrónicas.

Ejemplo de respuestas de Ejecutar Lambda sincrónicas

En los siguientes ejemplos se muestra la estructura de las respuestas de Ejecutar Lambda sincrónicas más comunes.

Example : quitar destinatarios especificados de un mensaje de correo electrónico

En el siguiente ejemplo se muestra la estructura de una respuesta de Ejecutar Lambda sincrónica para eliminar destinatarios de un mensaje de correo electrónico.

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

Example : rebote con un mensaje de correo electrónico personalizado

En el siguiente ejemplo se muestra la estructura de una respuesta de Ejecutar Lambda sincrónica para rebotar con un mensaje de correo electrónico personalizado.

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

Example : agregar destinatarios a un mensaje de correo electrónico

En el siguiente ejemplo se muestra la estructura de una respuesta de Ejecutar Lambda sincrónica para añadir destinatarios al mensaje de correo electrónico. Esto no actualiza los campos Para o CC del mensaje de correo electrónico.

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

```
}
```

Para obtener más ejemplos de código para usar al crear funciones de Lambda para las acciones de Run Lambda, consulte las plantillas de Amazon Lambda. WorkMail

Más información sobre el uso de Lambda con Amazon WorkMail

También puede acceder al contenido completo del mensaje de correo electrónico que activa la función de Lambda. Para obtener más información, consulte Recuperar el contenido de los mensajes con AWS Lambda.

Recuperar el contenido de los mensajes con AWS Lambda

Tras configurar una AWS Lambda función para gestionar los flujos de correo electrónico de Amazon WorkMail, puede acceder a todo el contenido de los mensajes de correo electrónico que se procesan con Lambda. Para obtener más información sobre cómo empezar a utilizar Lambda for Amazon WorkMail, consulte. Configuración AWS Lambda para Amazon WorkMail

Para acceder al contenido completo de los mensajes de correo electrónico, usa la `GetRawMessageContent` acción en la API Amazon WorkMail Message Flow. El ID de mensaje de correo electrónico que se transfiere a su función de Lambda en el momento de la invocación envía una solicitud a la API. A continuación, la API responde con el contenido MIME completo del mensaje de correo electrónico. Para obtener más información, consulta Amazon WorkMail Message Flow en la referencia de la WorkMail API de Amazon.

En el siguiente ejemplo se muestra cómo una función de Lambda que utiliza el entorno de tiempo de ejecución Python puede recuperar el contenido completo del mensaje.

> **Tip**
>
> Si comienza por implementar la función Lambda de Amazon WorkMail Hello World desde su cuenta, el AWS Serverless Application Repository sistema crea una función Lambda en su cuenta con todos los recursos y permisos necesarios. A continuación, puede añadir su lógica empresarial a la función de Lambda en función de su caso de 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)
```

Para ver ejemplos más detallados de cómo analizar el contenido de los mensajes que están en tránsito, consulte el amazon-workmail-lambda-templatesrepositorio en. GitHub

> **Note**
>
> Solo utilizas la API Amazon WorkMail Message Flow para acceder a los mensajes de correo electrónico en tránsito. Solo puede acceder a los mensajes en las 24 horas siguientes a su envío o recepción. Para acceder mediante programación a los mensajes del buzón de correo de un usuario, utilice uno de los otros protocolos compatibles con Amazon WorkMail, como IMAP o Exchange Web Services (EWS).

Actualización del contenido de los mensajes con AWS Lambda

Tras configurar una AWS Lambda función sincrónica para gestionar los flujos de correo electrónico, puede utilizar la `PutRawMessageContent` acción en la API de flujo de WorkMail mensajes de Amazon para actualizar el contenido de los mensajes de correo electrónico en tránsito. Para obtener más información sobre cómo empezar a utilizar las funciones de Lambda para Amazon WorkMail, consulte. Configuración de reglas de Ejecutar Lambda sincrónicas Para obtener más información sobre la API, consulte PutRawMessageContent.

> **Note**
>
> La PutRawMessageContent API requiere boto3 1.17.8, o puede añadir una capa a la función Lambda. Para descargar la versión correcta de boto3, consulta la página de boto en. GitHub Para obtener más información sobre cómo añadir capas, consulte Configuración de una función para utilizar capas.
>
> Este es un ejemplo de capa: `"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`. En este ejemplo, sustituya `${AWS::Region}` por una región de aws apropiada, como us-east-1.

> **Tip**
>
> Si comienza por implementar la función Lambda de Amazon WorkMail Hello World desde el AWS Serverless Application Repository en su cuenta, el sistema creará una función Lambda en su cuenta con los recursos y permisos necesarios. A continuación, puede añadir su lógica empresarial a la función de Lambda en función de sus casos de uso.

A medida que avance, recuerde lo siguiente:

- Utilice la GetRawMessageContentAPI para recuperar el contenido original del mensaje. Para obtener más información, consulte Recuperar el contenido de los mensajes con AWS Lambda.
- Una vez que tenga el mensaje original, cambie el contenido MIME. Cuando termine, suba el mensaje a un bucket de Amazon Simple Storage Service (Amazon S3) de su cuenta. Asegúrese de que el bucket de S3 utilice lo Cuenta de AWS mismo que sus WorkMail operaciones de Amazon y de que utilice la misma región de AWS que las llamadas a la API.
- Para WorkMail que Amazon procese las solicitudes, tu bucket de S3 debe tener la política correcta para poder acceder al objeto de S3. Para obtener más información, consulte Example S3 policy.
- Usa la PutRawMessageContentAPI para enviar el contenido actualizado del mensaje a Amazon WorkMail.

> **Note**
>
> La `PutRawMessageContent` API garantiza que el contenido MIME del mensaje actualizado cumpla con los estándares de la RFC, así como con los criterios mencionados en el tipo de RawMessageContentdatos. Los correos electrónicos entrantes a tu WorkMail organización de Amazon no siempre cumplen con esos estándares, por lo que la `PutRawMessageContent` API puede rechazarlos. En tales casos, puede consultar el mensaje de error devuelto para obtener más información sobre cómo solucionar cualquier problema.

Example Ejemplo de política 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/*"
                }
            }
        }
    ]
}
```

En el siguiente ejemplo se muestra cómo una función de Lambda utiliza el tiempo de ejecución de Python para actualizar el asunto de un mensaje de correo electrónico en tránsito.

```
    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)
```

Para ver más ejemplos de formas de analizar el contenido de los mensajes en tránsito, consulta el amazon-workmail-lambda-templatesrepositorio en. GitHub

Administrar el acceso a la API de Amazon WorkMail Message Flow

Utilice políticas AWS Identity and Access Management (IAM) para gestionar el acceso a la API de Amazon WorkMail Message Flow.

La API Amazon WorkMail Message Flow funciona con un único tipo de recurso, un mensaje de correo electrónico en tránsito. Cada mensaje de correo electrónico en tránsito tiene asociado un nombre de recurso de Amazon (ARN) único.

En el siguiente ejemplo se muestra la sintaxis de un ARN asociado a un mensaje de correo electrónico en tránsito.

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

Entre los campos que admiten cambios del ejemplo anterior se incluyen los siguientes:

- Región: la región de AWS de su WorkMail organización de Amazon.
- Cuenta: el Cuenta de AWS ID de tu WorkMail organización de Amazon.
- Organización: tu ID de WorkMail organización de Amazon.

- Contexto: indica si el mensaje es `incoming` o `outgoing` para su organización.
- ID de mensaje: el ID único del mensaje de correo electrónico que se transfiere como entrada a su función de Lambda.

El siguiente ejemplo incluye un IDs ejemplo de un ARN asociado a un mensaje de correo electrónico entrante en tránsito.

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

Puedes utilizarlos ARNs como recursos en la `Resource` sección de tus políticas de usuario de IAM para gestionar el acceso a WorkMail los mensajes de Amazon en tránsito.

Ejemplo de políticas de IAM para el acceso al flujo de WorkMail mensajes de Amazon

El siguiente ejemplo de política otorga a una entidad de IAM acceso de lectura completo a todos los mensajes entrantes y salientes de cada organización de Amazon de su WorkMail organización. Cuenta de AWS

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

Si tienes varias organizaciones Cuenta de AWS, también puedes limitar el acceso a una o más organizaciones. Esto resulta útil si determinadas funciones de Lambda solo deben utilizarse para determinadas organizaciones.

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

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

También puede elegir conceder acceso a mensajes dependiendo de si son `incoming` o `outgoing` de su organización. Para ello, use el calificador `incoming` o `outgoing` en el ARN.

La siguiente política de ejemplo concede acceso solo a mensajes entrantes de su organización.

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

El siguiente ejemplo de política otorga a una entidad de IAM acceso completo de lectura y actualización a todos los mensajes entrantes y salientes de cada organización de Amazon de su WorkMail organización. Cuentas de AWS

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

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

Comprobación de una regla de flujo de correo electrónico

Para comprobar la configuración actual de la regla, puede probar cómo se comporta la configuración con direcciones de correo electrónico específicas.

Para comprobar una regla de flujo de correo electrónico

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Organization settings (Configuración de la organización), Inbound/Outbound rules (Reglas de entrada y salida).
4. Junto a Test configuration (Probar configuración), escriba las direcciones de correo electrónico completas del remitente y el destinatario que desea probar.
5. Seleccione Probar. Se muestra la acción que se realizará para la dirección de correo electrónico proporcionada.

Eliminación de una regla de flujo de correo electrónico

Cuando elimina una regla de flujo de correo electrónico, los cambios se aplican de inmediato.

Para eliminar una regla de flujo de correo electrónico

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más

información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Organization settings (Configuración de la organización), Inbound/Outbound rules (Reglas de entrada y salida).
4. Seleccione la regla y elija Remove.
5. En el mensaje de confirmación, elija Remove (Eliminar).

Aplicación de políticas de DMARC en el correo electrónico entrante

Los dominios de correo electrónico utilizan registros del Sistema de Nombres de Dominio (DNS) para seguridad. Protegen a sus usuarios de ataques comunes como suplantación de identidad o el phishing. Los registros DNS suelen incluir registros de autenticación, notificación y conformidad de mensajes basados en dominios (DMARC) que el propietario del dominio que envía el correo electrónico establece. Los registros DMARC incluyen políticas que especifican las acciones que deben realizarse cuando un correo electrónico no supera una comprobación DMARC. Puede elegir si desea aplicar la política de DMARC en los correos electrónicos que se envían a su organización.

Las nuevas WorkMail organizaciones de Amazon tienen la aplicación de DMARC activada de forma predeterminada.

Para activar la aplicación DMARC

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Configuración de la organización. Aparece la página Configuración de la organización, que muestra un conjunto de pestañas.
4. Seleccione la pestaña DMARC y luego elija Editar.
5. Mueva el control deslizante Aplicación DMARC a la posición activado.

6. Selecciona la casilla situada junto a Reconozco que activar la aplicación del DMARC puede provocar que los correos electrónicos entrantes se eliminen o se pongan en cuarentena según la configuración del dominio del remitente.
7. Seleccione Save.

Para desactivar la aplicación DMARC

- Siga los pasos de la sección anterior, pero mueva el control deslizante Aplicación DMARC a la posición desactivado.

Uso del registro de eventos de correo electrónico para rastrear la aplicación DMARC

La activación de la aplicación DMARC puede provocar que los correos electrónicos entrantes se eliminen o se marquen como spam, en función de cómo haya configurado su dominio el remitente. Si un remitente configura incorrectamente su dominio de correo electrónico, es posible que los usuarios dejen de recibir correos electrónicos legítimos. Para comprobar si hay correos electrónicos que no se están entregando a tus usuarios, puedes habilitar el registro de eventos de correo electrónico para tu WorkMail organización de Amazon. A continuación, puede consultar los registros de eventos de correo electrónico para los correos electrónicos entrantes que se filtran en función de las políticas de DMARC del remitente.

Antes de utilizar el registro de eventos de correo electrónico para hacer un seguimiento de la aplicación de la DMARC, habilite el registro de eventos de correo electrónico en la WorkMail consola de Amazon. Para sacar el máximo provecho de los datos de registro, deje pasar algún tiempo mientras se registran los eventos de correo electrónico. Para obtener más información e instrucciones, consulte the section called “Activación del registro de eventos de correo electrónico”.

Para utilizar el registro de eventos de correo electrónico para realizar un seguimiento de la aplicación DMARC

1. En la consola de CloudWatch Insights, en Registros, selecciona Insights.
2. En Seleccionar grupo (s) de registros, selecciona el grupo de registros de tu WorkMail organización de Amazon. Por ejemplo,/aws/workmail/events/organization-alias.
3. Seleccione un período de tiempo para consultar.
4. Ejecute la siguiente consulta: stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. Elija Ejecutar consulta.

También puede configurar métricas personalizadas para estos eventos. Para obtener más información, consulte Creación de filtros de métricas.

Etiquetado de una organización

Etiquetar un recurso de una WorkMail organización de Amazon te permite:

- Diferencie entre las organizaciones en la Administración de facturación y costos de AWS consola.
- Controle el acceso a los recursos de WorkMail la organización de Amazon añadiéndolos al `Resource` elemento de las declaraciones de política de permisos AWS Identity and Access Management (IAM).

Para obtener más información sobre los permisos a WorkMail nivel de recursos de Amazon, consulte. Recursos Para obtener más información sobre el control de acceso basado en etiquetas, consulte Autorización basada en WorkMail etiquetas de Amazon.

WorkMail Los administradores de Amazon pueden etiquetar las organizaciones mediante la WorkMail consola de Amazon.

Para añadir etiquetas a una WorkMail organización de Amazon

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. Seleccione Tags (Etiquetas).
4. En Organization tags (Etiquetas de la organización), elija Add new tag (Agregar nueva etiqueta).
5. En Clave, introduzca un nombre que identifique la etiqueta.
6. (Opcional) En Value (Valor), escriba un valor para la etiqueta.
7. (Opcional) Repita los pasos 4 a 6 para agregar más etiquetas a la organización. Puede añadir hasta 50 etiquetas.
8. Elija Guardar para guardar los cambios.

Puedes ver las etiquetas de tu organización en la WorkMail consola de Amazon.

Los desarrolladores también pueden etiquetar las organizaciones mediante el AWS SDK o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte los `UntagResource` comandos `TagResourceListTagsForResource`, y en Amazon WorkMail API Reference o AWS CLI Command Reference.

Puedes eliminar etiquetas de una organización en cualquier momento mediante la WorkMail consola de Amazon.

Para eliminar etiquetas de una WorkMail organización de Amazon

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. Seleccione Tags (Etiquetas).
4. En Organization tags (Etiquetas de la organización), elija la opción Remove (Quitar) situada junto a la etiqueta que desee quitar.
5. Elija Enviar para guardar los cambios.

Uso de reglas de control de acceso

Las reglas de control de acceso de Amazon WorkMail permiten a los administradores controlar la forma en que los usuarios y los roles de suplantación de identidad de su organización tienen acceso a Amazon. WorkMail Cada WorkMail organización de Amazon tiene una regla de control de acceso predeterminada que otorga acceso al buzón a todos los usuarios y roles de suplantación de identidad añadidos a la organización, independientemente del protocolo de acceso o la dirección IP que utilicen. Los administradores pueden editar o reemplazar la regla predeterminada por una de las suyas, agregar una nueva regla o eliminar una regla.

> **Warning**
>
> Si un administrador elimina todas las reglas de control de acceso de una organización, Amazon WorkMail bloquea todo el acceso a los buzones de la organización.

Los administradores pueden aplicar reglas de control de acceso que permitan o denieguen el acceso según los siguientes criterios:

- Protocolos: el protocolo utilizado para acceder al buzón de correo. Algunos ejemplos son Autodiscover, EWS, IMAP, SMTP ActiveSync, Outlook para Windows y Webmail.
- Direcciones IP: los rangos de IPv4 CIDR utilizados para acceder al buzón.
- WorkMail Usuarios de Amazon: los usuarios de su organización que se utilizan para acceder al buzón.
- Roles de suplantación: los roles de suplantación de su organización que se utilizan para acceder al buzón de correo. Para obtener más información, consulte Administración de roles de suplantación.

Los administradores aplican reglas de control de acceso además de los permisos de buzón y carpeta del usuario. Para obtener más información, consulta Uso de los permisos del buzón de correo Compartir carpetas y permisos de carpetas en la Guía del WorkMail usuario de Amazon.

> **Note**
>
> - Al habilitar el acceso de Outlook para Windows, se recomienda habilitar también el acceso a Autodiscover y EWS.
> - Las reglas de control de acceso no se aplican al acceso a WorkMail la consola Amazon o al SDK. En su lugar, utilice roles o políticas AWS Identity and Access Management (de IAM). Para obtener más información, consulte Gestión de identidades y accesos para Amazon WorkMail.

Creación de reglas de control de acceso

Crea nuevas reglas de control de acceso desde la WorkMail consola de Amazon.

Para crear una nueva regla de control de acceso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. Elija Access control rules (Reglas de control de acceso).
4. Seleccione Creación de regla.
5. En Description (Descripción), escriba una descripción para la regla.
6. En Efecto, elija Permitir o Denegar. Esto permite o deniega el acceso en función de las condiciones que seleccione en el paso siguiente.
7. En Esta regla se aplica a las solicitudes que..., seleccione las condiciones que desee aplicar a la regla, como por ejemplo si desea incluir o excluir protocolos, direcciones IP o usuarios específicos, o roles de suplantación.
8. (Opcional) Si introduce rangos de direcciones IP, usuarios o roles de suplantación, seleccione Añadir para añadirlos a la regla.
9. Seleccione Creación de regla.

Edición de reglas de control de acceso

Edita las reglas de control de acceso nuevas y predeterminadas desde la WorkMail consola de Amazon.

Para editar una regla de control de acceso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. Elija Access control rules (Reglas de control de acceso).
4. Seleccione la regla que desea editar.
5. Elija Edit rule.
6. Edite la descripción, el efecto y las condiciones según sea necesario.
7. Seleccione Save changes (Guardar cambios).

> **Important**
>
> Al cambiar una regla de acceso, los buzones de correo afectados podrían tardar cinco minutos en seguir la regla actualizada. Los clientes que acceden a los buzones afectados podrían mostrar un comportamiento incoherente durante ese periodo. Sin embargo, verá de inmediato un comportamiento correcto al probar sus reglas. Para obtener más información sobre las pruebas de reglas, consulte los pasos en la siguiente sección.

Prueba de reglas de control de acceso

Para ver cómo se aplican las reglas de control de acceso de tu organización, prueba las reglas desde la WorkMail consola de Amazon.

Para probar las reglas de control de acceso para su organización

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. Elija Access control rules (Reglas de control de acceso).
4. Elija Test rules (Probar reglas).
5. En Request context (Contexto de solicitud), seleccione el protocolo que se va a probar.

6. En Source IP address (Dirección IP de origen), escriba la dirección IP que se va a probar.
7. En Solicitud realizada por, elija Usuario o Rol de suplantación para realizar la prueba.
8. Seleccione Usuario o Rol de suplantación para probar.
9. Seleccione Probar.

Los resultados de la prueba aparecen en Effect (Efecto).

Eliminación de reglas de control de acceso

Elimina las reglas de control de acceso que ya no necesites de la WorkMail consola de Amazon.

> **Warning**
>
> Si un administrador elimina todas las reglas de control de acceso de una organización, Amazon WorkMail bloquea todo el acceso a los buzones de la organización.

Para eliminar una regla de control de acceso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. Elija Access control rules (Reglas de control de acceso).
4. Seleccione la regla que desea eliminar.
5. Elija Delete rule (Eliminar regla).
6. Elija Eliminar.

Establecimiento de políticas de retención de buzones de correo

Puedes establecer políticas de retención de buzones para tu WorkMail organización de Amazon. Las políticas de retención eliminan automáticamente los mensajes de correo electrónico de los buzones

de correo de los usuarios tras un periodo de tiempo que usted elija. Puede elegir a qué carpetas de buzón de correo aplicar las políticas de retención. Además, puede elegir si desea establecer políticas de retención diferentes para las distintas carpetas. Las políticas de retención de buzones de correo se aplican a las carpetas seleccionadas en todos los buzones de correo de usuario de la organización. Los usuarios no pueden anular las políticas de retención.

Para establecer una política de retención de buzones de correo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. Elija Política de retención.
4. Para Acciones de carpeta, junto a cada carpeta de buzón de correo que desee incluir en la política, seleccione Eliminar o Eliminar permanentemente.
5. Introduzca el número de días que desea conservar los mensajes de correo electrónico en cada carpeta de buzón de correo antes de eliminarlos.
6. Seleccione Save.

Deje transcurrir 48 horas para que las políticas de retención de su organización se apliquen. Si eliges la acción Eliminar carpeta, los usuarios pueden recuperar los mensajes de correo electrónico eliminados de la aplicación WorkMail web de Amazon y de los clientes compatibles. Si elige la acción de carpeta Eliminar permanentemente, los mensajes de correo electrónico no se podrán recuperar una vez eliminados.

El número de días que una política de retención conserva un elemento se basa en cuándo se creó, modificó o movió. Por ejemplo, si una política de retención elimina elementos después de un año, la política cuenta los días de retención a partir de la fecha en que se creó o realizó la última acción sobre ese elemento. No se ve afectado por la fecha en que implementó la política de retención.

Uso de dominios

Puedes configurar Amazon WorkMail para que utilice un dominio personalizado. También puede hacer que un dominio sea el predeterminado para su organización y habilitarlo AutoDiscover para Microsoft Outlook.

Temas

Adición de un dominio

Puedes añadir hasta 100 dominios a tu WorkMail organización de Amazon. Al añadir un nuevo dominio, se añade automáticamente una política de autorización de envío de Amazon Simple Email Service (Amazon SES) a la política de identidad del dominio. Esto proporciona a Amazon WorkMail acceso a todas las acciones de envío de Amazon SES de tu dominio y te permite redirigir el correo electrónico a tu dominio. También puede redirigir el correo electrónico a dominios externos.

> **Note**
>
> Como práctica recomendada, debería añadir alias para `<postmaster@>` y `<abuse@>` a todos sus dominios. Puede crear grupos de distribución para estos alias si desea que usuarios específicos de su organización reciban el correo enviado a estos alias.

Cuando configures tu WorkMail organización de Amazon con un dominio personalizado, recuerda lo siguiente acerca de los registros DNS de tu dominio:

- Para los registros MX y CNAME de detección automática, recomendamos establecer el valor de Tiempo de vida (TTL) en 3600. Reducir el TTL garantiza que sus servidores de correo no utilicen registros MX obsoletos o no válidos después de que actualice dichos registros o migre sus buzones de correo.
- Tras crear los usuarios y los grupos de distribución y, a continuación, migrar correctamente los buzones, debes actualizar el registro MX para empezar a reenviar correos electrónicos a Amazon. WorkMail Las actualizaciones de los registros de DNS puede tardar hasta 48 horas en procesarse.
- Algunos proveedores de DNS añaden automáticamente los nombres de dominio al final de los registros DNS. Si añade un registro que ya contiene el nombre de dominio, como _amazonses.example.com, es posible que el nombre de dominio se duplique y aparezca _amazonses.example.com.example.com. Para evitar la duplicación del nombre de dominio en el nombre de registro, añada un punto al final del nombre de dominio en el registro de DNS. Esto indica a su proveedor de DNS que el nombre de registro está totalmente cualificado y ya no es relativo al nombre de dominio. También impide que el proveedor de DNS añada un nombre de dominio adicional.
- Los nombres de registro copiados incluyen el nombre de dominio. En función del proveedor del servicio DNS que utilice, es posible que el nombre de dominio ya se haya añadido al registro de DNS del dominio.
- Tras crear un registro DNS, selecciona el icono de actualización en la WorkMail consola de Amazon para ver el estado de la verificación y el valor del registro. Para obtener más información sobre la verificación de dominios, consulte Verificación de dominios.
- Le recomendamos que configure su dominio como el dominio `MAIL FROM`. AutoDiscover Para habilitarlo en dispositivos iOS, debe configurar su dominio como `MAIL FROM` dominio. Puede ver el estado de su dominio `MAIL FROM` en la sección Mejora de la capacidad de entrega de la consola. Para obtener más información, consulte Configuración de un dominio MAIL FROM personalizado.

Para añadir un dominio

1. Inicia sesión en la WorkMail consola de Amazon AWS Management Console y ábrela en https://console.aws.amazon.com/workmail/.
2. Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más

información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

3. En el panel de navegación, elija Organizaciones y, a continuación, seleccione el nombre de la organización a la que desea añadir un dominio.
4. En el panel de navegación, elija Dominios y, a continuación, Añadir dominio.
5. En la pantalla Añadir dominio, introduzca un nombre de dominio. Los nombres de dominio solo pueden contener caracteres latinos básicos (ASCII).

> **Note**
>
> Si tiene un dominio que se administra en una zona alojada pública de Amazon Route 53, puede elegirlo en el menú desplegable que aparece al introducir un nombre de dominio.

6. Elija Añadir dominio.

Aparece una página que enumera los registros DNS del nuevo dominio. La página agrupa los registros en las siguientes secciones:

- Propiedad del dominio
- WorkMail configuración
- Seguridad mejorada
- Entrega de correo electrónico mejorada

Cada una de estas secciones contiene uno o más registros DNS, y cada registro muestra un valor Estado. En la siguiente lista se muestran los registros y sus valores de estado disponibles.

Propiedad de TXT

Verificado: registro resuelto y verificado.

Pendiente: registro aún no verificado.

Fallido: no se ha podido verificar la propiedad. Registro no coincidente o inaccesible.

WorkMail Configuración MX

Verificado: registro resuelto y verificado.

Faltante: no se ha podido resolver el registro.

Inconsistente: el valor no coincide con el registro esperado.

AutoDiscover

Verificado: registro resuelto y verificado.

Faltante: no se ha podido resolver el registro.

Inconsistente: el valor no coincide con el registro esperado.

> **Note**
>
> El proceso AutoDiscover de verificación también comprueba que la AutoDiscover configuración sea correcta. El proceso verifica los ajustes de configuración de cada fase. Cuando la verificación finaliza, aparece una marca de verificación verde junto a Verificado en la columna Estado. Puede pasar el ratón por encima de Verificado y ver cuál de las fases fue verificada por el proceso. Para obtener más información sobre las AutoDiscover fases, consulte AutoDiscover Habilitar la configuración de puntos finales.

DKIM CNAME

Verificado: registro resuelto y verificado.

Pendiente: registro aún no verificado.

Fallido: no se ha podido verificar la propiedad. Registro no coincidente o inaccesible.

Para obtener más información sobre la firma DKIM, consulte Autenticación de correo electrónico con DKIM en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

SPF TXT

Verificado: registro resuelto y verificado.

Faltante: no se ha podido resolver el registro.

Inconsistente: el valor no coincide con el registro esperado.

Para obtener más información sobre la verificación SPF, consulta Autenticación de correo electrónico con SPF.

DMARC TXT

Verificado: registro resuelto y verificado.

Faltante: no se ha podido resolver el registro.

Inconsistente: el valor no coincide con el registro esperado.

Para obtener más información sobre los registros DMARC en Amazon WorkMail, consulte Cumplimiento de DMARC con Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

Dominio TXT MAIL FROM

Verificado: registro resuelto y verificado.

Pendiente: registro aún no verificado.

Fallido: no se ha podido verificar la propiedad. Registro no coincidente o inaccesible.

Dominio MX MAIL FROM

Verificado: registro resuelto y verificado.

Faltante: no se ha podido resolver el registro.

Inconsistente: el valor no coincide con el registro esperado.

7. En el siguiente paso, elija la acción apropiada en función del proveedor de DNS que utilice.

Si usa un dominio de Route 53

- En la parte superior de la página, elija Actualizar todo en Route 53.

Si utiliza otro proveedor de DNS

- Copie los registros y péguelos en su proveedor de DNS. Puede copiar los registros en bloque o de uno en uno. Para copiar registros en bloque, elija Copiar todo. Esto crea una zona de archivos que puede importar a su proveedor de DNS. Para copiar los registros de uno en uno,

elija los cuadrados superpuestos junto al nombre del registro y, a continuación, pegue cada uno de ellos en su proveedor de DNS.

8. Elija el icono de actualización para actualizar el Estado de cada registro. Esto verifica la propiedad del dominio y la correcta configuración de tu dominio con Amazon WorkMail.

Eliminación de un dominio

Puede eliminar un dominio cuando ya no lo necesite. Sin embargo, primero debe eliminar a las personas o grupos que utilicen el dominio como dirección de correo electrónico.

Para eliminar un dominio

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Nombre de región y puntos de conexión en Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En la lista de dominios, seleccione la casilla de verificación junto al nombre de dominio y, a continuación, elija Remove.
4. En el cuadro de diálogo Eliminar dominio, escriba el nombre del dominio que desee eliminar y elija Eliminar.

Elección del dominio predeterminado

Puede hacer que un dominio asociado a su organización sea el predeterminado para los usuarios y grupos de esa organización. Convertir un dominio en predeterminado no cambia las direcciones de correo electrónico existentes.

Para convertir un dominio en predeterminado

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más

información, consulte Nombre de región y puntos de conexión en Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En la lista de dominios, marque la casilla de verificación situada junto al nombre de dominio que desee utilizar y elija Configurar como predeterminado.

Verificación de dominios

Debes verificar tu dominio después de añadirlo a la WorkMail consola de Amazon. La verificación del dominio confirma que eres el propietario del dominio y que utilizarás Amazon WorkMail como servicio de correo electrónico para el dominio.

Para verificar un dominio, añada registros TXT y MX en su servicio DNS. Los registros TXT le habilitan para añadir notas a su servicio DNS. Los registros MX especifican el servidor de correo entrante.

Utiliza la consola Amazon SES para crear los registros TXT y MX y, a continuación, utiliza la WorkMail consola de Amazon para añadir los registros a su servicio de DNS. Siga estos pasos.

Creación de registros TXT y MX

1. Abra la consola Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, elija Dominios y, a continuación, Verificar un nuevo dominio.

   Aparece el cuadro de diálogo Verificar un nuevo dominio.
3. En el cuadro Dominio, introduzca el nombre del dominio que creó en la sección Adición de un dominio.
4. (Opcional) Si desea utilizar el correo DomainKeys identificado (DKIM), seleccione la casilla Generar configuración de DKIM.
5. Elija Verificar este dominio.

   La consola muestra una lista de registros TXT y MX.
6. Seleccione el enlace Descargar conjunto de registros como CSV que se encuentra bajo el listado TXT.

Aparece el cuadro de diálogo Guardar como. Elija una ubicación para la descarga y, a continuación, elija Guardar.

7. Abra el archivo CSV descargado y copie todo su contenido.

Una vez creados los registros TXT y MX, añádalos a su proveedor de DNS. En los siguientes pasos se utiliza Route 53. Si utiliza un proveedor de DNS diferente y no sabe cómo añadir registros, consulte la documentación de su proveedor.

1. Inicie sesión en la consola de Route 53 AWS Management Console y ábrala en. https://console.aws.amazon.com/route53/
2. En el panel de navegación, elija Hosted Zones. A continuación, elija el botón de opción situado junto al dominio que desee verificar.
3. En la lista de registros DNS de su dominio, elija Importar archivo de zona.
4. En Archivo de zona, pegue los registros copiados en el cuadro de texto. Aparece una lista de los archivos debajo del cuadro de texto.
5. Desplácese hasta el final de la lista y elija Importar.

> **Note**
>
> Espere hasta 72 horas para que el proceso de verificación se complete.

Verificación de registros TXT y registros MX con su servicio DNS

Confirme que el registro TXT que verifica que usted es el propietario del dominio se añade correctamente a su servicio DNS. Este procedimiento utiliza la herramienta nslookup, que está disponible para Windows y Linux. En Linux, también puede utilizar dig.

Para utilizar la herramienta `nslookup`, primero debe encontrar los servidores DNS que sirven a su dominio. A continuación, consulte esos servidores para ver los registros TXT. Puede consultar los servidores DNS de su dominio porque esos servidores son los que contienen la mayor cantidad de up-to-date información de su dominio. Esta información puede tardar tiempo en propagarse a otros servidores DNS.

Uso de nslookup para verificar que su registro TXT se haya añadido a su servicio DNS

1. Localice los servidores de nombres de su dominio:

   a. Abra un símbolo del sistema (Windows) o un terminal (Linux).

   b. Ejecute el siguiente comando para obtener una lista de todos los servidores de nombres que sirven a su dominio. *example.com*Sustitúyalos por tu dominio.

   ```
   nslookup -type=NS example.com
   ```

   En el siguiente paso consultará uno de estos servidores de nombres.

2. Comprueba que el registro WorkMail TXT de Amazon se ha añadido correctamente.

   a. Ejecuta el siguiente comando y *example.com* sustitúyelo por tu dominio y *ns1.name-server.net* por un servidor de nombres del paso 1.

   ```
   nslookup -type=TXT _amazonses.example.com ns1.name-server.net
   ```

   b. Revise la cadena `"text ="` que aparece en la salida de nslookup. Confirma que esta cadena coincide con el valor TXT de tu dominio en la lista de remitentes verificados de la WorkMail consola de Amazon.

   En el siguiente ejemplo, desea ver un registro TXT para _amazonses.example.com con un valor de `fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk=`. Si actualiza el registro correctamente, el comando muestra la siguiente salida:

   ```
   _amazonses.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
   ```

Uso de dig para verificar que el registro TXT se haya añadido al servicio DNS

1. Abra una sesión de terminal.
2. Ejecute el siguiente comando para obtener una lista de los registros TXT de su dominio. *example.com*Sustitúyelo por tu dominio.

   ```
   dig +short example.com txt
   ```

3. Comprueba que la cadena que aparece a continuación TXT en el resultado del comando coincide con el valor TXT que ves al seleccionar el dominio en la lista de remitentes verificados de la WorkMail consola de Amazon.

Para utilizar nslookup para comprobar que el registro MX se ha añadido a su servicio DNS

1. Busque los servidores de nombres del dominio:

   a. Abra un símbolo del sistema.

   b. Ejecute el siguiente comando para obtener una lista de todos los servidores de nombres de su dominio.

   ```
   nslookup -type=NS example.com
   ```

   En el siguiente paso consultará uno de estos servidores de nombres.

2. Compruebe que el registro MX se ha añadido correctamente:

   a. Ejecuta el siguiente comando y *example.com* sustitúyelo por tu dominio y *ns1.name-server.net* por uno de los servidores de nombres que identificaste en el paso anterior.

   ```
   nslookup -type=MX example.com ns1.name-server.net
   ```

   b. En la salida del comando, verifique que la cadena que sigue a `mail exchange =` coincida con uno de los siguientes valores:

   Región Este de EE. UU. (Norte de Virginia) — `10 inbound-smtp.us-east-1.amazonaws.com`

   Región Oeste de EE. UU (Oregón) — `10 inbound-smtp.us-west-2.amazonaws.com`

   Región Europa (Irlanda) — `10 inbound-smtp.eu-west-1.amazonaws.com`

   > **Note**
   >
   > `10` representa el número de preferencia o prioridad de MX.

Para utilizar dig para comprobar que su registro MX se haya añadido a su servicio DNS

1. Abra una sesión de terminal.
2. Ejecute el siguiente comando para obtener una lista de los registros MX de su dominio.

```
dig +short example.com mx
```

3. Compruebe que la cadena que sigue a `MX` coincide con uno de los siguientes valores:

   Región Este de EE. UU. (Norte de Virginia) — `10 inbound-smtp.us-east-1.amazonaws.com`

   Región Oeste de EE. UU (Oregón) — `10 inbound-smtp.us-west-2.amazonaws.com`

   Región Europa (Irlanda) — `10 inbound-smtp.eu-west-1.amazonaws.com`

   > **Note**
   >
   > `10` representa el número de preferencia o prioridad de MX.

Solución de problemas de verificación de dominios

Para solucionar problemas comunes con la verificación de dominios, consulte las siguientes sugerencias:

Su servicio DNS no permite guiones bajos en los nombres de registro TXT

Omita `_amazonses` en el nombre del registro TXT.

Quiere verificar el mismo dominio varias veces pero no puede tener varios registros TXT con el mismo nombre

Si su servicio DNS no le permite tener varios registros TXT con el mismo nombre, utilice cualquiera de las siguientes soluciones:

- (Recomendado) Si su servicio DNS lo permite, asigne múltiples valores al registro TXT. Por ejemplo, si su DNS está administrado por Amazon Route 53, puede configurar múltiples valores para el mismo registro TXT de la siguiente manera:
  1. En la consola de Route 53, elija el registro TXT `_amazonses` que añadió al verificar su dominio en la primera región.

2. En Valor, pulse Intro después del primer valor.
3. Añada el valor para la región adicional y guarde el conjunto de registros.

- Si solo necesita verificar su dominio dos veces, puede verificarlo una vez creando un registro TXT con `_amazonses` en el nombre y, a continuación, creando otro registro sin `_amazonses` en el nombre del registro.

La WorkMail consola de Amazon informa que la verificación del dominio ha fallado

Amazon no WorkMail encuentra el registro TXT necesario para tu servicio de DNS. Compruebe si el registro TXT necesario se ha añadido correctamente a su servicio DNS según el procedimiento descrito en Verificación de registros TXT y registros MX con su servicio DNS.

Su proveedor de DNS ha añadido el nombre de dominio al final del registro TXT

Añadir un registro TXT que ya contiene el nombre de dominio, como _amazonses.example.com, puede dar lugar a la duplicación del nombre de dominio, como _amazonses.example.com.example.com. Para evitar la duplicación del nombre de dominio, añada un punto al final del nombre de dominio en el registro TXT. Esto indica a su proveedor de DNS que el nombre del registro está totalmente cualificado y ya tiene el nombre de dominio incluido en el registro TXT.

Amazon WorkMail informa que el registro MX no es coherente

Al migrar desde servidores de correo existentes, el registro MX podría devolver un estado de Inconsistente. Actualiza tu registro MX para que apunte a Amazon WorkMail en lugar de apuntar a tu servidor de correo anterior. El registro MX también se devuelve como incoherente cuando se utiliza un proxy de correo electrónico de terceros junto con Amazon WorkMail. Si este es el caso, se puede ignorar la advertencia Inconsistent (Incoherente) sin problemas.

AutoDiscover Habilitar la configuración de puntos finales

AutoDiscover le permite configurar Microsoft Outlook y los clientes móviles utilizando únicamente su dirección de correo electrónico y contraseña. El servicio mantiene una conexión con Amazon WorkMail y actualiza la configuración local cada vez que cambias los puntos de conexión o la configuración. Además, AutoDiscover permite a tu cliente utilizar WorkMail funciones adicionales de Amazon, como la libreta de direcciones sin conexión, el Out-of-Office Asistente y la posibilidad de ver las horas libres o ocupadas en el Calendario.

El cliente realiza las siguientes AutoDiscover fases para detectar el punto final del servidor: URLs

- Fase 1: el cliente realiza una búsqueda de Protocolo de Copia Segura (SCP) en el Active Directory local. Si su cliente no está unido a un dominio, AutoDiscover omita este paso.
- Fase 2: el cliente envía una solicitud a la siguiente dirección URLs y valida los resultados. Estos puntos de conexión solo están disponibles si se utiliza HTTPS.
  - https:///autodiscover/autodiscover.xml *company.tld*
  - https://autodiscover. *company.tld*/autodiscover/autodiscover.xml
- Fase 3: El cliente realiza una búsqueda DNS en autodiscover.company.tld y envía una solicitud GET no autenticada al punto de conexión derivado desde la dirección de correo electrónico del usuario. Si el servidor devuelve una redirección 302, el cliente vuelve a enviar la AutoDiscover solicitud al punto final HTTPS devuelto.

Si todas estas fases fallasen, el cliente no se podrá configurar automáticamente. Para obtener información sobre la configuración manual de dispositivos móviles, consulte Configurar manualmente el dispositivo.

Cuando añadas tu dominio a Amazon, se te solicitará que añadas el registro AutoDiscover DNS a tu proveedor WorkMail. Esto permite al cliente realizar la fase 3 del AutoDiscover proceso. Sin embargo, estos pasos no funcionan en todos los dispositivos móviles, como la aplicación de correo electrónico stock de Android. Como resultado, es posible que deba configurar AutoDiscover la fase 2 manualmente.

Puedes usar los siguientes métodos para configurar la AutoDiscover fase 2 para tu dominio:

(Recomendado) Usa Route 53 y Amazon CloudFront

> **Note**
>
> En los siguientes pasos se explica cómo crear un proxy para https://autodiscover. *company.tld*/autodiscover/autodiscover.xml. Para crear un proxy para https://*company.tld*/autodiscover/autodiscover.xml, elimine el `autodiscover.` prefijo de los dominios en los siguientes pasos.
> El uso CloudFront de Route 53 puede conllevar gastos. Para obtener más información sobre los precios aplicables, consulte los CloudFront precios de Amazon y los precios de Amazon Route 53.

Para habilitar AutoDiscover la fase 2 con Route 53 y CloudFront

1. Obtenga un certificado SSL para la detección automática. *company.tld*y cárguelo en AWS Identity and Access Management (IAM) o. AWS Certificate Manager Para obtener más información, consulte Uso de certificados de servidor en la Guía del usuario de IAM, o Introducción en la Guía del usuario de AWS Certificate Manager .
2. Crea una nueva CloudFront distribución:
   1. Abra la CloudFront consola enhttps://console.aws.amazon.com/cloudfront/v4/home.
   2. En el panel de navegación, elija Distribuciones.
   3. Elija Crear distribución.
   4. En Web, elija Introducción.
   5. En Configuración de origen, introduzca los siguientes valores:
      - Nombre de dominio de origen: el nombre de dominio apropiado para su región:
        - Este de EE. UU. (Norte de Virginia) — **`autodiscover-service.mail.us-east-1.awsapps.com`**
        - Oeste de EE. UU. (Oregón) — **`autodiscover-service.mail.us-west-2.awsapps.com`**
        - Europa (Irlanda) — **`autodiscover-service.mail.eu-west-1.awsapps.com`**
      - Política de protocolo de origen: la política deseada: **`Match Viewer`**

      > **Note**
      >
      > Deje Ruta de origen en blanco. No cambie el valor autorrellenado de ID de origen.

   6. En Configuración predeterminada de comportamiento de la caché, seleccione los siguientes valores para los ajustes enumerados:
      - Viewer Protocol Policy: solo HTTPS
      - Allowed HTTP Methods: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
      - Cache Based on Selected Request Headers: All (Almacenar en caché en función de los encabezados de solicitud seleccionados: Todo)
      - Forward Cookies: todas
      - Query String Forwarding and Caching: None (Improves Caching) [Reenvío de cadenas de consulta y almacenamiento en caché: Ninguno (mejora el almacenamiento en caché)]

- Smooth Streaming: no
- Restrict Viewer Access: no

7. Seleccione los valores siguientes para Distribution Settings (Configuración de distribución):
   - Price Class: usar solo Estados Unidos, Canadá y Europa
   - Para nombres de dominio alternativos (CNAMEs), introduzca **`autodiscover.`*`company.tld`*** o***`company.tld`***, dónde *`company.tld`* está su nombre de dominio.
   - Certificado SSL: certificado SSL personalizado (almacenado en IAM)
   - Custom SSL Client Support (Soporte de cliente SSL personalizado): elija All Clients (Todos los clientes) u Only Clients that Support Server Name Indication (SNI) (Solo clientes que admiten indicación de nombre de servidor, SNI). Es posible que las versiones anteriores de Android no funcionen con esta última opción.

     > **Note**
     >
     > Si elige All Clients (Todos los clientes), deje Default Root Object (Objeto raíz predeterminado) en blanco.

   - Logging (Registro): elija On (Activado) u Off (Desactivado). Activado habilita el registro.
   - En Comment (Comentario), escriba **`AutoDiscover type2 for autodiscover.`*`company.tld`***
   - Estado de distribución: elija Habilitado.
8. Elija Crear distribución.

3. En la consola de Route 53, cree un registro que dirija el tráfico de Internet de su nombre de dominio a su CloudFront distribución.

   > **Note**
   >
   > En estos pasos se asume que el registro DNS de example.com está alojado en Route 53. Si no utiliza Route 53, siga los procedimientos de la consola de administración de su proveedor de DNS.

   1. En el panel de navegación de la consola, elija Zonas alojadas y, a continuación, elija un dominio.

2. En la lista de dominios, elija el nombre de dominio que desee utilizar.
3. En Registros, elija Crear registro.
4. En Crear registro rápido, establezca los siguientes parámetros:
   - En Nombre del registro, introduzca un nombre para el registro.
   - En Política de enrutamiento, seleccione Enrutamiento sencillo.
   - Mueva el control deslizante Alias para activarlo. El control deslizante cambia a azul en estado activado.
   - En la lista Tipo de registro, elija A: Dirige el tráfico a una IPv4 dirección y a algunos recursos de AWS.
   - En la lista Enrutar el tráfico a la distribución, elija Alias a la CloudFront distribución.
   - Aparece un cuadro de búsqueda bajo la lista Enrutar tráfico a. Introduzca el nombre de la CloudFront distribución en el cuadro de texto. También puede seleccionar su distribución en la lista que aparece al seleccionar el cuadro de búsqueda.
5. Elija Crear registro.

Uso de un servidor web Apache

Los siguientes pasos explican cómo usar un servidor web Apache para crear un proxy para https://autodiscover.*company.tld*/autodiscover/autodiscover.xml. Para crear un proxy para https://*company.tld*/autodiscover/autodiscover.xml, elimine la «detección automática». en los siguientes pasos.

Para habilitar AutoDiscover la fase 2 con un servidor web Apache

1. Ejecute las siguientes directivas en un servidor Apache habilitado para SSL:

   ```
   SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-
   service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
   ```

2. Según sea necesario, habilite los siguientes módulos de Apache. Si desconoce cómo hacerlo, consulte la ayuda de Apache:

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`

- `ssl`

Consulte la siguiente sección para obtener información sobre las pruebas y la solución de problemas AutoDiscover.

AutoDiscover fase 2: solución de problemas

Una vez que hayas configurado tu proveedor de DNS AutoDiscover, puedes probar la configuración de tu AutoDiscover punto final. Si ha configurado correctamente su punto de conexión, este responderá con un mensaje de solicitud no autorizada.

Para realizar una solicitud básica no autorizada

1. Desde un terminal, crea una solicitud POST no autenticada para el AutoDiscover punto final.

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ```

   Si su punto de conexión está configurado correctamente, debería devolver un mensaje `401 unauthorized`, como se muestra en el siguiente ejemplo:

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ...
   HTTP/1.1 401 Unauthorized
   ```

2. A continuación, prueba una solicitud real. AutoDiscover Cree un archivo `request.xml` con el siguiente contenido 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. Utilice el `request.xml` archivo que creó y envíe una AutoDiscover solicitud autenticada al punto final. Recuerde sustituirlo por *`testuser@company.tld`* una dirección de correo electrónico válida:

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

La respuesta tendrá un aspecto similar al siguiente ejemplo si el punto de conexión está configurado correctamente:

```
$ 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>
```

Modificación de políticas de identidad de dominios

Las políticas de identidad de dominio especifican permisos para acciones de correo electrónico, como redirigir mensajes de correo electrónico. Por ejemplo, puedes redirigir los correos electrónicos a cualquier dirección de correo electrónico de tu WorkMail organización de Amazon.

> **Note**
>
> A partir del 1 de abril de 2022, Amazon WorkMail comenzó a utilizar los directores de servicio para la autorización en lugar de los directores de AWS cuenta. Si agregaste un dominio antes del 1 de abril de 2022, es posible que tengas una política anterior que utilice un principal de AWS cuenta para la autorización. De ser así, le recomendamos que actualice a la política más reciente. Los pasos de esta sección explican cómo hacerlo. Su organización seguirá enviando correos electrónicos con normalidad durante la actualización.

Solo debe seguir estos pasos si no utiliza una política personalizada de Amazon SES. Si utiliza una política personalizada de Amazon SES, deberá actualizarla usted mismo. Para obtener más información, consulte Política personalizada de entidad principal de servicio de Amazon SES, más adelante en este tema.

> **Important**
>
> No elimine sus dominios existentes. Si lo hace, interrumpirá el servicio de correo. Lo único que debe hacer es volver a introducir sus dominios existentes.

Para actualizar una política de identidad de dominios

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. Para ello, abra la lista Seleccionar una región situada a la derecha del cuadro de búsqueda y elija la región deseada. Para obtener más información sobre las regiones, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, el nombre de su organización.
3. En el panel de navegación, elija Dominios.

4. Resalte y copie el nombre del dominio que desea volver a introducir y, a continuación, elija Añadir dominio.

   Aparece el cuadro de diálogo Añadir dominio.
5. Pegue el nombre copiado en el cuadro Nombre de dominio y, a continuación, elija Añadir dominio.
6. Repita los pasos 3-5 para el resto de dominios de su organización.

Política personalizada de entidad principal de servicio de Amazon SES

Si utiliza una política personalizada de Amazon SES, adapte este ejemplo para utilizarlo en su 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"
        }
      }
    }
  ]
}
```

Autenticación de correo electrónico con SPF

El marco de directivas de remitente (SPF) es un estándar de validación de correo electrónico diseñado para combatir la suplantación de correo electrónico. La suplantación de identidad

(spoofing) es el acto de hacer que un correo electrónico enviado por un actor malicioso parezca provenir de un usuario legítimo. Para obtener información sobre cómo configurar el SPF para su dominio WorkMail habilitado para Amazon, consulte Autenticación del correo electrónico con SPF en Amazon SES.

Configuración de un dominio MAIL FROM personalizado

De forma predeterminada, Amazon WorkMail usa un subdominio de amazonses.com como `MAIL FROM` dominio para el correo saliente. Esto puede provocar fallos de entrega si la política DMARC de su dominio solo está configurada para SPF. Para resolver este problema, configure su propio dominio como dominio `MAIL FROM`. Para obtener información sobre cómo configurar su dominio de correo electrónico como dominio `MAIL FROM`, consulte Configuración de un dominio MAIL FROM personalizado en la Guía para desarrolladores de Amazon Simple Email Service.

> **Important**
>
> Se requiere un dominio MAIL FROM personalizado cuando se habilita AutoDiscover para dispositivos iOS.

Para obtener más información sobre los dominios `MAIL FROM` personalizados, consulte Amazon SES ahora admite dominios MAIL FROM personalizados.

Uso de los usuarios

Puedes crear y eliminar usuarios de Amazon WorkMail. Además, puede restablecer sus contraseñas de correo electrónico, administrar sus cuotas de buzón de correo y acceso a dispositivos, y controlar sus permisos de buzón de correo.

Temas

Ver una lista de usuarios

Para ver la lista de usuarios

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, seleccione Usuarios.
4. Además, puede filtrar los usuarios por nombre de usuario, nombre para mostrar o dirección de correo electrónico principal.

> **Note**
>
> La búsqueda distingue entre mayúsculas y minúsculas.

Agregar un usuario

Cuando añades un usuario, Amazon crea WorkMail automáticamente buzones para él. Los usuarios pueden iniciar sesión y acceder a su correo desde la aplicación WorkMail web de Amazon, su dispositivo móvil o mediante Microsoft Outlook en macOS o PC.

Para añadir un usuario

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, seleccione la organización a la que desea añadir usuarios.
3. En el panel de navegación, elija Usuarios y, a continuación, elija Agregar usuario.

   Aparece la pantalla Añadir un usuario.
4. En Detalles del usuario, en el campo Nombre de usuario, introduzca el nombre del usuario. El nombre también aparece en el cuadro Dirección de correo electrónico. Si desea que el usuario tenga una dirección de correo electrónico distinta de su nombre de usuario, puede editar el campo Dirección de correo electrónico.
5. (Opcional) Introduzca el nombre y apellido del usuario en los cuadros Nombre y Apellido.
6. En el cuadro Nombre para mostrar, introduzca el nombre para mostrar del usuario.
7. En el cuadro Dirección de correo electrónico, acepte el alias de correo electrónico o introduzca otro.
8. De forma predeterminada, los usuarios aparecen en la lista global de direcciones. Para ocultar al usuario de la lista global de direcciones, desactive la casilla Mostrar en la lista global de direcciones.
9. Seleccione No crear un buzón para añadir un usuario como usuario remoto a la organización.

10. En Configuración de contraseña, introduzca la contraseña del usuario en los cuadros Contraseña y Repita la contraseña.
11. Elija Añadir usuario.

Habilitar usuarios

Cuando integras Amazon WorkMail con tu Active Directory corporativo, o si ya tienes usuarios disponibles en tu directorio Simple AD, puedes habilitar esos usuarios en Amazon WorkMail. Siga también estos pasos para volver a habilitar un usuario cuya cuenta haya sido deshabilitada.

Para habilitar usuarios

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija la organización para la cual desea habilitar usuarios.
3. En el panel de navegación, elija Usuarios.

   Aparece una lista de usuarios. En la lista se visualizan las cuentas de usuario en los estados habilitado, deshabilitado y usuario del sistema.
4. En la lista de usuarios con cuentas deshabilitadas, active las casillas de verificación de los usuarios que desee habilitar y, a continuación, elija Habilitar.

   Aparece el cuadro de diálogo Habilitar usuarios.
5. Según sea necesario, revise y cambie la dirección de correo electrónico principal de cada usuario y, a continuación, elija Habilitar.

Administrar los alias de los usuarios

Puedes añadir o eliminar los alias de correo electrónico de los usuarios.

Para añadir un alias de correo electrónico a un usuario

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de la organización para la que quiere añadir usuarios.
3. En el panel de navegación, elija Usuarios y, a continuación, seleccione el nombre del usuario al que quiere añadir un alias.
4. En la sección Detalles del usuario, seleccione la pestaña Alias.
5. En la pestaña Alias, selecciona Añadir alias.
6. En el cuadro Alias, introduce un alias.
7. Seleccione un dominio para un alias.
8. Elija Agregar.

Para eliminar un alias de correo electrónico de un usuario

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de la organización de la que quiere eliminar usuarios.
3. En el panel de navegación, elija Usuarios y, a continuación, seleccione el nombre del usuario del que quiere eliminar los alias.
4. En la sección Detalles del usuario, seleccione la pestaña Alias.
5. En la pestaña Alias, active la casilla de verificación situada junto a los alias que desee eliminar.
6. Compruebe los alias que se eliminarán.
7. En la ventana Eliminar alias, selecciona Eliminar.

Deshabilitación de usuarios

Puede deshabilitar a cualquier usuario de una organización en cualquier momento. Al deshabilitar un usuario, se vuelve inaccesible de inmediato. A los usuarios que estén inhabilitados durante más de 30 días se les eliminará su bandeja de entrada de Amazon WorkMail.

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, seleccione Organizaciones y, a continuación, elija la organización que contiene los usuarios que desea deshabilitar.
3. En el panel de navegación, seleccione Usuarios.

   Aparece una lista de todos los usuarios que muestra las cuentas en los estados habilitado, deshabilitado y usuario del sistema.
4. En la lista de usuarios habilitados, active las casillas de verificación de las cuentas que desee deshabilitar y, a continuación, elija Desactivar.

   Aparece el cuadro de diálogo Deshabilitar usuarios.
5. Elija Deshabilitar.

Modificación de los detalles de los usuarios

Al editar los detalles del usuario, puedes cambiar lo siguiente:

- Datos personales: nombres, direcciones de correo electrónico, números de teléfono y otros datos personales.
- Cuotas de buzón de correo (tamaños): las cuotas pueden oscilar entre 1 MB y 51 200 MB (50 GB). Amazon WorkMail notifica a los usuarios cuando alcanzan el 90 por ciento de su cuota. Además, cambiar la cuota del buzón de correo de un usuario no afecta a los precios. Para obtener más información sobre los precios, consulta Amazon WorkMail Pricing.
- Acceso de dispositivos móviles: elimine dispositivos o datos de los mismos y consulte sus detalles.
- Permisos de acceso al buzón de correo: conceda a los usuarios permiso para utilizar un buzón de correo y otorgue a los usuarios diferentes niveles de acceso al mismo.

- Tokens de acceso personal (cuando el IAM Identity Center está activado): permite ver y eliminar los tokens de acceso personal.

> **Note**
>
> Si integras Amazon WorkMail con un directorio de AD Connector, no podrás editar estos detalles desde AWS Management Console. En su lugar, debe editarlos mediante sus herramientas de administración de Active Directory. Las limitaciones se aplican cuando su organización está en modo de interoperabilidad. Para obtener más información, consulte Limitaciones en modo de interoperabilidad.

Para editar los detalles del usuario

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija la organización que desee utilizar.
3. En el panel de navegación, elija Usuarios y, a continuación, elija el nombre del usuario que desee editar.

Para editar datos personales

1. En la sección Detalles del usuario, elija Editar.
2. En Detalles del usuario, introduzca o modifique la información personal del usuario según sea necesario.
3. Cuando haya finalizado, elija Guardar cambios.

Para asociarse con un usuario del Centro de Identidad de IAM

1. En Detalles del usuario, seleccione Editar.

2. Introduzca el seudónimo del usuario del IAM Identity Center al que desee asociar. Puede ver esta información en la tabla Usuarios asignados de la página del Centro de identidad de IAM o en la consola del Centro de identidades de IAM.
3. Elija Guardar cambios.

Para editar las cuotas de buzones de correo

1. En Detalles del usuario, elija la pestaña Cuota y, a continuación, Editar.
2. En el cuadro Actualizar cuota de buzón de correo, introduzca un tamaño para el buzón de correo. Puede especificar valores entre **1** y **51200**.
3. Elija Guardar cambios.

Para administrar datos de dispositivos móviles

> **Note**
>
> Para gestionar los dispositivos móviles, tus usuarios primero tienen que conectar sus dispositivos a tu instancia de Amazon WorkMail. Para obtener información sobre la conexión de dispositivos móviles, consulta Configuración de clientes de dispositivos móviles para Amazon WorkMail.

1. En Detalles del usuario, elija la pestaña Dispositivos móviles.
2. Para ver una lista actualizada de dispositivos, elija Actualizar.
3. Para ver los detalles de un dispositivo, elija el nombre del dispositivo en la columna ID de dispositivo.
4. Para eliminar un dispositivo o eliminar los datos del mismo, elija el botón de opción situado junto al nombre del dispositivo y, a continuación, elija Eliminar o Eliminar datos según sea necesario.
5. En el cuadro de diálogo que aparece, confirme la operación de eliminación o eliminación de datos. Recuerda que los usuarios volverán a aparecer cuando sincronicen sus dispositivos con Amazon de WorkMail nuevo.

Para editar permisos de buzón de correo

1. Elija la pestaña Permisos.

2. Haga una de las siguientes acciones:

    1. Para añadir permisos, elija Añadir permisos. Abra la lista Añadir nuevos permisos y elija un usuario o grupo, elija la configuración de permisos para el usuario o grupo y, a continuación, elija Guardar.
    2. Para editar los permisos de los usuarios, selecciona el botón situado junto al nombre del usuario. Elija Editar, luego las opciones que desee y finalmente Guardar.

    Para obtener más información sobre las opciones de permisos, consulte Uso de los permisos del buzón de correo.

3. Para eliminar todos los permisos, elija Eliminar y, a continuación, confirma la eliminación.

Para eliminar los tokens de acceso personales

> **Note**
>
> Asegúrese de que ningún cliente de correo electrónico utilice activamente el token que va a eliminar. Al eliminar un token cuando está en uso, se interrumpirá la autenticación de los clientes que lo utilizan.

1. Seleccione la pestaña Tokens de acceso personal.
2. En la lista de tokens de acceso personal, seleccione el token de acceso personal que desee eliminar.
3. Selecciona Eliminar token.
4. Introduzca Type en el cuadro de texto de confirmación.

Restablecer la contraseña del usuario

Si un usuario olvida su contraseña o tiene problemas para iniciar sesión en Amazon WorkMail, puedes restablecerla.

> **Note**
>
> - Si ha integrado Amazon WorkMail con un directorio de AD Connector, debe restablecer la contraseña de usuario en Active Directory.
> - Si has integrado Amazon WorkMail con el Centro de Identidad de IAM, puedes optar por restablecer la contraseña del usuario. Para obtener más información, consulte Restablecer la contraseña de usuario del Centro de Identidad de IAM para un usuario final en la Guía del AWS IAM Identity Center usuario.

Restablecimiento de una contraseña de usuario

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, seleccione Usuarios.
4. En la lista de usuarios, active la casilla de verificación situada junto al nombre del usuario y, a continuación, seleccione Restablecer contraseña.
5. En el cuadro de diálogo Restablecer contraseña, introduzca la nueva contraseña y, a continuación, elija Restablecer.

Solución de problemas de las políticas de WorkMail contraseñas de Amazon

Si no se puede restablecer la contraseña, compruebe que la nueva contraseña cumple los requisitos de las políticas de contraseñas.

Los requisitos de la política de contraseñas dependen del tipo de directorio que utilice tu WorkMail organización de Amazon.

Política de contraseñas para el WorkMail directorio Amazon y el directorio Simple AD

De forma predeterminada, las contraseñas de un WorkMail directorio de Amazon o de un directorio Simple AD deben ser:

- No estar vacías
- Tener al menos ocho caracteres
- Tener menos de 64 caracteres
- Estar compuestas de caracteres Basic Latin o Latin-1

Las contraseñas también debe contener caracteres de tres de los cinco grupos siguientes:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Dígitos numéricos (0 a 9)
- Caracteres especiales (como <, ~ o !)
- Caracteres del complemento Latin-1 (como é, ü o ñ)

Las políticas WorkMail de contraseñas del directorio de Amazon no se pueden cambiar.

Para cambiar una política de contraseñas de Simple AD, utilice las herramientas de administración de AD en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) Windows de su directorio de Simple AD. Para obtener más información, consulte Instalación de herramientas de administración de Active Directory en la Guía de administración de AWS Directory Service .

AWS Managed Microsoft AD Política de contraseñas de directorios

Para obtener información sobre la política de contraseñas predeterminada para un directorio AWS Managed Microsoft AD , consulte Administración de políticas de contraseñas para AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service .

Política de contraseñas del conector AD

El conector AD utiliza la política de contraseñas del dominio de Active Directory al que se conecta. Consulte la documentación de su dominio de Active Directory para obtener más información sobre la configuración de la política de contraseñas.

Uso de notificaciones

Con la API de notificaciones WorkMail push de Amazon, puede recibir notificaciones automáticas sobre los cambios en su buzón de correo, incluidas las nuevas actualizaciones de correo electrónico y calendario. Debe registrar a las personas URLs (o a las personas que responden a las notificaciones automáticas) para recibir las notificaciones. Con esta función, los desarrolladores pueden crear aplicaciones adaptables para WorkMail los usuarios de Amazon, ya que las aplicaciones reciben notificaciones rápidas sobre los cambios desde el buzón de correo de un usuario.

Para obtener más información, consulte Suscripciones de notificación, eventos del buzón y EWS en Exchange.

Puede suscribirse a carpetas específicas, como Bandeja de entrada o Calendario, o a todas las carpetas para los eventos de cambio de buzón de correo (incluyendo Nuevo correo, Creado y Modificado).

Puede utilizar bibliotecas de cliente como la API Java de EWS o la API C# de EWS administrada para acceder a esta característica. En la página encontrará un ejemplo completo de una aplicación de respuesta automática desarrollada con AWS Lambda y API Gateway (con el marco AWS Serverless). AWS GitHub La aplicación utiliza la API Java de EWS.

A continuación, se incluye una solicitud de suscripción push de ejemplo:

```
<?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>
```

A continuación, se incluye el resultado de una solicitud de suscripción enviada correctamente:

```
<?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>
```

A continuación, las notificaciones se envían a la URL especificada en la solicitud de suscripción. A continuación, se muestra una notificación de ejemplo:

```
<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>
```

Para confirmar que el agente de respuesta de la notificación de inserción ha recibido la notificación, debe responder con lo siguiente:

```
<?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>
```

Para cancelar la suscripción de recepción de notificaciones de inserción, los clientes deben enviar una respuesta de cancelación de la suscripción en el campo `SubscriptionStatus`, similar a la siguiente:

```
<?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>
```

Para comprobar el estado de tu respondedor de notificaciones push, Amazon WorkMail envía un «latido» (también denominado a`StatusEvent`). La frecuencia con la que se envían las notificaciones la determina el parámetro `StatusFrequency` proporcionado en la solicitud de suscripción inicial. Por ejemplo, si `StatusFrequency` es igual a **1**, se envía un `StatusEvent` cada 1 minuto. Este valor puede oscilar entre 1 y 1440 minutos. Este `StatusEvent` tiene el siguiente aspecto:

```
<?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>
```

Si un agente de respuesta de notificación push de un cliente no responde con el mismo estado 0K que antes, la notificación se vuelve a intentar durante un máximo de `StatusFrequency` minutos. Por ejemplo, si `StatusFrequency` equivale a 5 y la primera notificación no se envía, se reintenta durante un máximo de 5 minutos con un retroceso exponencial entre cada reintento. Si la notificación no se entrega una vez transcurrido el tiempo de reintento, la suscripción se invalida y no se envían nuevas notificaciones. Debe crear una nueva suscripción para continuar recibiendo notificaciones de eventos del buzón de correo. Actualmente, puede suscribirse a un máximo de tres suscripciones por buzón de correo.

Habilitación del correo electrónico firmado o cifrado

Puede utilizar S/MIME para habilitar a los usuarios para que envíen correo electrónico firmado o cifrado tanto dentro como fuera de la organización.

> **Note**
>
> Los certificados de usuario de la lista de global de direcciones (GAL) se admite solo en una configuración de Active Directory conectada.

Para habilitar usuarios para enviar correos electrónicos firmados o cifrados

1. Configure un conector de Active Directory (AD). La configuración de un conector AD con su directorio en las instalaciones permite a los usuarios continuar usando sus credenciales corporativas existentes.
2. Configure la autoinscripción de certificados para emitir y almacenar certificados de usuario automáticamente en el directorio activo. Amazon WorkMail recibe los certificados de usuario de Active Directory y los publica en la GAL. Para obtener más información, consulte Configure Certificate Autoenrollment.
3. Distribuya los certificados generados a los usuarios exportándolos desde el servidor que ejecuta Microsoft Exchange y enviándolos por correo.

4. Cada usuario instala el certificado en su programa de correo electrónico (como Windows Outlook) y dispositivos móviles.

Uso de grupos

Puedes usar grupos como listas de distribución en Amazon WorkMail para recibir correos electrónicos de direcciones de correo electrónico genéricas, como `<sales@example.com>` o `<support@example.com>`. Puede crear varios alias de correo electrónico para un grupo.

También puede utilizar los grupos como grupos de seguridad para compartir un buzón de correo o un calendario con un determinado equipo.

Los grupos no tienen buzones de correo propios y eso afecta a los permisos de buzón de correo que puede conceder a un grupo. Para obtener información sobre cómo configurar los permisos de buzón de correo para un grupo, consulte Administración de permisos del buzón de correo para grupos.

> **Note**
>
> Pueden ser necesarias hasta dos horas para que los grupos recién añadidos aparezcan en la libreta de direcciones sin conexión de Microsoft Outlook.

Temas

Ver una lista de grupos

Para ver la lista de grupos

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Grupos.
4. Además, puede filtrar los grupos por nombre de grupo o dirección de correo electrónico principal.

> **Note**
>
> La búsqueda distingue entre mayúsculas y minúsculas.

Añadir un grupo

Puedes añadir grupos desde la WorkMail consola de Amazon.

Para añadir un grupo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   De ser necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccionar una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, selecciona Grupos y, a continuación, selecciona Añadir grupo.

   Aparece la página Agregar grupo.
4. En Nombre del grupo, introduzca un nombre para el grupo.
5. En Dirección de correo electrónico, introduzca la dirección de correo electrónico principal del grupo.
6. Verifica la dirección de correo electrónico del grupo y actualízala según sea necesario.

7. De forma predeterminada, el grupo se muestra en la lista global de direcciones. Para ocultar el grupo de la lista global de direcciones, desactive la casilla Mostrar en la lista global de direcciones.
8. Elija Añadir grupo.

Habilitar grupos

Cuando integras Amazon WorkMail con tu Active Directory corporativo, o si ya tienes grupos disponibles en tu Active Directory simple, puedes usar esos grupos como grupos de seguridad o listas de distribución en Amazon WorkMail.

Para activar un grupo de un directorio existente

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Grupos.
4. Seleccione la casilla de verificación situada junto al grupo que desee activar y, a continuación, seleccione Activar.

   Aparece el cuadro de diálogo Habilitar grupos, que le pedirá que confirme la operación.
5. Según sea necesario, revisa y cambia la dirección de correo electrónico principal de cada grupo y, a continuación, selecciona Activar.

Añadir miembros a un grupo

Después de crear y habilitar un WorkMail grupo de Amazon, usa la WorkMail consola de Amazon para añadir miembros a ese grupo.

> **Note**
>
> Si Amazon WorkMail está integrado con un servicio de Active Directory conectado o Microsoft Active Directory, puede usar Active Directory para administrar los miembros de su grupo. Sin embargo, los cambios pueden tardar más en propagarse a Amazon WorkMail.

Para añadir miembros a un grupo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Grupos.
4. Seleccione el nombre del grupo.
5. En la página de detalles del grupo, selecciona la pestaña Miembros.
6. Elija un grupo o usuario para añadirlo en Grupo o usuario.
7. Seleccione el usuario o grupo en el menú desplegable.
8. Seleccione Guardar.

Los cambios podrían tardar unos minutos en propagarse.

Edición de los detalles del grupo

Puedes editar los detalles de un grupo.

Para editar los detalles del grupo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más

información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, selecciona Grupos y, a continuación, selecciona el grupo que deseas editar.
4. En la página de detalles del grupo, actualice la dirección de correo electrónico según sea necesario.
5. De forma predeterminada, los grupos se muestran en la lista global de direcciones. Para ocultar el grupo de la lista global de direcciones, desactive la casilla Mostrar en la lista global de direcciones.
6. Elija Guardar cambios.

Eliminar miembros de un grupo

Usa la WorkMail consola de Amazon para eliminar miembros de un grupo.

> **Note**
>
> Si Amazon WorkMail está integrado con un Active Directory o Microsoft Active Directory conectado, puede usar Active Directory para administrar los miembros de su grupo. Sin embargo, si lo hace, puede crear el tiempo necesario para propagar los cambios a Amazon WorkMail.

Para eliminar miembros de un grupo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Grupos y, a continuación, elija el nombre del grupo.

4. En la página de detalles del grupo, selecciona la pestaña Miembros.
5. Seleccione el miembro que desee eliminar del grupo.
6. Elija Eliminar.

Los cambios podrían tardar unos minutos en propagarse.

Administrar los alias de los grupos

Puedes añadir o eliminar alias de correo electrónico de los grupos.

Para añadir un alias de correo electrónico a un grupo.

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de la organización para la que desee añadir un alias.
3. En el panel de navegación, elija Grupos y, a continuación, seleccione el nombre del grupo al que desee añadir un alias.
4. En la sección de detalles del grupo, elija Alias.
5. En Alias, selecciona Añadir alias.
6. En el cuadro Alias, introduce un alias.
7. Seleccione un dominio para un alias.
8. Elija Agregar.

Para eliminar un alias de correo electrónico de un grupo.

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de la organización de la que quiere eliminar un alias.
3. En el panel de navegación, elija Grupos y, a continuación, seleccione el nombre del grupo del que quiere eliminar los alias.
4. En la sección de detalles del grupo, elija Alias.
5. En Alias, active la casilla de verificación situada junto a los alias que desee eliminar.
6. Elija Eliminar.
7. Compruebe los alias que se eliminarán.
8. En la ventana Eliminar alias, selecciona Eliminar.

Desactivar grupos

Cuando ya no necesite un grupo, puede desactivarlo.

Para desactivar un grupo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Grupos.
4. En Nombre del grupo, seleccione los grupos que desee deshabilitar y, a continuación, elija Desactivar.
5. En el cuadro de diálogo Deshabilitar grupos, elija Deshabilitar.

Eliminación de un grupo

Para poder eliminar un grupo, primero debe deshabilitarlo. Para obtener más información sobre la deshabilitación de grupos, consulte Desactivar grupos.

Para eliminar un grupo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Grupos.
4. Seleccione la casilla de verificación situada junto al grupo deshabilitado que desee eliminar y elija Eliminar.

   Aparece el cuadro de diálogo Eliminar.
5. En el cuadro Introduzca el nombre del grupo para confirmar la eliminación, introduzca el nombre del grupo y, a continuación, seleccione Eliminar.

> **Note**
>
> Para eliminar un grupo de forma permanente, usa la acción de la `DeleteGroup` API para Amazon WorkMail. Para obtener más información, consulta DeleteGroupla referencia de la WorkMail API de Amazon.

Uso de recursos

Amazon WorkMail puede ayudar a tus usuarios a reservar recursos. Por ejemplo, los usuarios pueden reservar salas de reuniones o equipos como proyectores, teléfonos o coches. Para reservar un recurso, el usuario lo añade a la invitación a la reunión.

Temas

Ver una lista de recursos

Para ver la lista de recursos

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Recursos.
4. Además, puede filtrar los recursos por nombre del recurso o dirección de correo electrónico principal.

> **Note**
>
> La búsqueda distingue entre mayúsculas y minúsculas.

Añadir un recurso

Puede añadir un nuevo recurso a su organización y permitir que sus usuarios lo reserven.

Para añadir un recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, selecciona Recursos y, a continuación, Añadir recurso.

   Aparece la página Agregar recurso.
4. En el cuadro Nombre del recurso, introduzca un nombre para el recurso.
5. Si lo desea, en el cuadro Descripción del recurso, introduzca una descripción para el recurso.
6. En Tipo de recurso, elija una opción.
7. Compruebe la dirección de correo electrónico del recurso y actualícela según sea necesario.
8. De forma predeterminada, el recurso se muestra en la lista global de direcciones. Para ocultar el recurso de la lista global de direcciones, desactive la casilla Mostrar en la lista global de direcciones.
9. Seleccione Add resource (Añadir recurso).

Edición de detalles de un recurso

Puedes editar los detalles generales de un recurso, como el nombre, la descripción, el tipo y la dirección de correo electrónico, las opciones de reserva y los delegados.

Para editar detalles generales de un recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Resources y, a continuación, seleccione el recurso que desea editar.
4. En la página de detalles del recurso, actualiza el nombre, la descripción, el tipo de recurso o la dirección de correo electrónico del recurso según sea necesario.
5. De forma predeterminada, los recursos se muestran en la lista global de direcciones. Para ocultar el recurso de la lista global de direcciones, desactive la casilla Mostrar en la lista global de direcciones.
6. Elija Guardar cambios.

Puede configurar un recurso para que acepte o rechace solicitudes de reserva de forma automática.

Puede editar las opciones de reserva del recurso.

Para cambiar las opciones de reserva de un recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Resources y, a continuación, seleccione el recurso que desea editar. Aparece una página que muestra los detalles del recurso.
4. En Opciones de reserva, selecciona Editar.
5. Según sea necesario, selecciona o desmarca la casilla de verificación situada junto a una opción para activarla o desactivarla.

> **Note**
>
> Al deshabilitar cualquiera de las opciones de reserva automática, deberá crear un delegado que se encargue de las solicitudes de reserva. En los pasos siguientes se explica cómo crear un delegado.

Puede añadir un delegado para controlar las solicitudes de reserva de un recurso que no tenga configuradas las opciones de reserva automática. Los delegados de recursos reciben automáticamente copias de todas las solicitudes de reserva y tienen acceso completo al calendario de recursos. Además, tienen que aceptar todas las solicitudes de reserva para un recurso.

Para añadir un delegado de recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Recursos y, a continuación, seleccione el nombre del recurso al que desea añadir un delegado.
4. (Opcional) En la pestaña Opciones de reserva, selecciona Editar, desactiva la casilla Aceptar automáticamente todas las solicitudes de recursos y, a continuación, selecciona Guardar.
5. Elija la pestaña Delegados y, a continuación, Añadir delegado.

   Aparece el cuadro de diálogo Añadir delegado.
6. Abra la lista Buscar delegados y elija un delegado, después elija Guardar.

Para eliminar un delegado de recursos

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de la organización de la que quiere eliminar a los delegados.
3. En el panel de navegación, elija Recursos y, a continuación, seleccione el nombre del recurso del que quiere eliminar un delegado.
4. Elija Delegados y, a continuación, elija el delegado que desee eliminar.
5. Elija Eliminar.

Administrar los alias de los recursos

Puedes añadir o eliminar alias de correo electrónico a los recursos.

Para añadir un alias de correo electrónico a un recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de la organización a la que desee añadir un alias.
3. En el panel de navegación, elija Recursos y, a continuación, seleccione el nombre del recurso al que desee agregar un alias.
4. En la sección Detalles del recurso, elija Alias.
5. En Alias, selecciona Añadir alias.
6. En el cuadro Alias, introduce un alias.
7. Seleccione un dominio para un alias.
8. Elija Agregar.

Para eliminar un alias de correo electrónico de un recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizations y, a continuación, elija el nombre de la organización de la que quiere eliminar los alias.
3. En el panel de navegación, elija Recursos y, a continuación, seleccione el nombre del recurso del que quiere eliminar los alias.
4. En la sección Detalles del recurso, elija Alias.
5. En Alias, active la casilla de verificación situada junto a los alias que desee eliminar.
6. Elija Eliminar.
7. Compruebe los alias que se eliminarán.
8. En la ventana Eliminar alias, selecciona Eliminar.

Habilitación de un recurso

De forma predeterminada, Amazon WorkMail crea un recurso. Si tú o alguien más deshabilita un recurso, puedes volver a activarlo en un plazo de 30 días.

Para habilitar un recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información sobre las regiones, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, seleccione Organizaciones y, a continuación, elija la organización que contiene el recurso que desea habilitar.
3. En el panel de navegación, elija Recursos.
4. En la lista de recursos, seleccione el botón situado junto al recurso que desea habilitar y, a continuación, elija Habilitar.

Aparece el cuadro de diálogo Habilitar recurso.

5. Elija Habilitar.

Deshabilitación de un recurso

Al deshabilitar un recurso, lo deja indisponible para reserva. Por ejemplo, puede deshabilitar una sala de conferencias mientras se remodela y habilitarla una vez que esté disponible para su uso.

Para deshabilitar un recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información sobre las regiones, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, seleccione Organizaciones y, a continuación, elija la organización que contiene el recurso que desea deshabilitar.
3. En el panel de navegación, elija Recursos.
4. En la lista de recursos, seleccione el botón situado junto al recurso que desea deshabilitar y, a continuación, elija Deshabilitar.

   Aparece el cuadro de diálogo Deshabilitar recurso.
5. Elija Deshabilitar.

Eliminación de un recurso

Cuando ya no necesite un recurso, puede eliminarlo. Sin embargo, primero debe deshabilitar el recurso. Para obtener información sobre cómo deshabilitar un recurso, consulte los pasos en la sección anterior.

Para eliminar un recurso

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información sobre las regiones, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizaciones y, a continuación, elija la organización deseada.
3. En el panel de navegación, elija Recursos.
4. En la lista de recursos, seleccione el botón situado junto al recurso deshabilitado que desea eliminar y, a continuación, elija Eliminar.

   Aparece el cuadro de diálogo Eliminar recurso.
5. En el cuadro Introducir el nombre del recurso para confirmar la eliminación, introduzca el nombre del recurso que desea eliminar y, a continuación, elija Eliminar recurso.

Trabajar con IAM Identity Center

Para habilitar la autenticación multifactorial (MFA) en Amazon, asocie sus usuarios de WorkMail Amazon al Centro de WorkMail Identidad de IAM. Para obtener más información, consulte ¿Qué es el Centro de Identidad de IAM?

En la siguiente tabla se describen los pasos para abordar diferentes escenarios.

Escenario	Pasos
Asociación de WorkMail usuarios de Amazon al centro de identidad de IAM	1. Habilitación del centro de identidad de IAM en Amazon WorkMail 2. Asignación de usuarios y grupos del Centro de Identidad de IAM a la aplicación Amazon WorkMail 3. Asociación de usuarios de Amazon con WorkMail usuarios del Centro de Identidad de IAM
WorkMail Usuarios actuales de Amazon	1. Cree usuarios del IAM Identity Center con el mismo nombre de usuario, agrupe los usuarios y asígnelos a la WorkMail aplicació n Amazon. 2. Asocie los usuarios de Amazon a WorkMail los usuarios del Centro de Identidad de IAM.
Usuarios actuales del Centro de Identidad de IAM	1. Cree WorkMail usuarios de Amazon con el mismo nombre de usuario que los usuarios del IAM Identity Center. 2. Asigne los usuarios o grupos del Centro de Identidad de IAM a la WorkMail aplicación Amazon. 3. Asocie los usuarios de Amazon a WorkMail los usuarios del Centro de Identidad de IAM.

Escenario	Pasos
Conexión de un directorio externo al Centro de Identidad de IAM	1. Sincronice los usuarios del directorio externo con el grupo del Centro de Identidad de IAM. Para obtener más información, consulte los tutoriales sobre las fuentes de identidad de IAM Identity Center 2. Asigne el grupo de centros de identidad de IAM a la WorkMail aplicación Amazon. 3. Conecta el directorio externo a Amazon WorkMail y asegúrate de que los nombres de usuario coincidan 4. Asocie los usuarios de Amazon a WorkMail los usuarios del Centro de Identidad de IAM.

Una vez completados los pasos anteriores, podrá ver el estado del Centro de Identidad de IAM, el enlace al Centro de Identidad de AWS IAM para gestionar los usuarios y los grupos, la URL de la aplicación web de WorkMail Amazon habilitada para MFA, el modo de autenticación, el estado del token de acceso personal y el cronograma en el Centro de Identidad de IAM en Configuración de la consola de Amazon. WorkMail Para obtener más información sobre la administración de MFA en la consola del IAM Identity Center, consulte Autenticación multifactor para los usuarios del IAM Identity Center.

> **Note**
>
> Asegúrese de que la configuración entre Amazon WorkMail e IAM Identity Center esté bien probada y verificada. Los usuarios podrían perder el acceso a sus buzones si la configuración no es correcta y no está completa.

Temas

- Habilitación del centro de identidad de IAM en Amazon WorkMail
- Asignación de usuarios y grupos del Centro de Identidad de IAM a la aplicación Amazon WorkMail
- Asociación de usuarios de Amazon con WorkMail usuarios del Centro de Identidad de IAM
- Modo de autenticación

- Configuración de los tokens de acceso personal
- Desactivar el Centro de identidad de IAM

Habilitación del centro de identidad de IAM en Amazon WorkMail

Cuando habilitas el Centro de Identidad de IAM, actúa como capa de autenticación para los WorkMail usuarios de Amazon. Los usuarios del IAM Identity Center se gestionan por separado del WorkMail directorio de Amazon. Se recomienda utilizar los mismos nombres de usuario en IAM Identity Center y Amazon. WorkMail

> **Note**
>
> Asegúrese de que Amazon WorkMail e IAM Identity Center estén configurados en la misma región.

Para activar el Centro de identidades de IAM, sigue estos pasos.

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, selecciona Identity Center.

   Aparece la página de configuración del IAM Identity Center.
3. Seleccione Habilitar.

   Aparece la ventana Activar el centro de identidad de IAM.
4. Seleccione Habilitar.

   Aparece la página de configuración del Identity Center con el estado del Identity Center.
5. Para añadir usuarios y grupos del Centro de Identidad de IAM a su WorkMail organización de Amazon, siga el enlace que aparece debajo del estado del Centro de identidades. Para obtener información sobre cómo añadir usuarios y grupos, consulte Administrar identidades en el Centro de identidades de IAM. .

Asignación de usuarios y grupos del Centro de Identidad de IAM a la aplicación Amazon WorkMail

Al activar el Centro de Identidad de IAM en Amazon WorkMail, WorkMail crea una aplicación en el Centro de Identidad de IAM en tu nombre. De forma predeterminada, los usuarios del Centro de Identidad de IAM deben estar asignados a esta aplicación o pertenecer a un grupo que esté asignado a esta aplicación para poder acceder a un buzón de correo de la WorkMail organización de Amazon. Para obtener más información, consulte las aplicaciones AWS gestionadas en la Guía del AWS IAM Identity Center usuario.

Puede asignar usuarios y grupos del Centro de identidades de IAM a Amazon WorkMail de las siguientes maneras:

- Por usuarios del Centro de Identidad de IAM: puede asignar usuarios del Centro de Identidad de IAM a Amazon. WorkMail
- Por grupo de centros de identidad de IAM: puede asignar grupos de centros de identidad de IAM a Amazon. WorkMail Al añadir un grupo, todos los usuarios de un grupo tendrán acceso a Amazon WorkMail.

  Para obtener más información sobre cómo añadir usuarios y grupos, consulte Usuarios, grupos y aprovisionamiento en el Centro de identidades de IAM.

> **Note**
>
> Si va a conectar su fuente de identidad actual con el Centro de identidades de IAM, revise lo siguiente antes de cambiar la fuente de directorio.
>
> - El Centro de Identidad de IAM gestiona su autenticación.
> - Amazon WorkMail conservará todos los WorkMail usuarios y grupos de Amazon.
> - El Centro de Identidad de IAM conservará todos los usuarios, grupos y tareas del Centro de Identidad de IAM.
> - Debe gestionar WorkMail los usuarios y grupos de Amazon en la WorkMail consola de Amazon.
> - Debe gestionar los usuarios y grupos del Centro de Identidad de IAM en el Centro de Identidad de IAM.

- Los usuarios sin una asignación de IAM Identity Center o una asociación de usuarios no pueden acceder a Amazon WorkMail.
- Debe gestionar los controles de políticas de MFA en IAM Identity Center.
- Al cambiar la fuente del Centro de Identidad de IAM a Administrar Active Directory en el Centro de Identidad de IAM, debe deshabilitar las configuraciones existentes del Centro de Identidad de IAM en Amazon WorkMail y volver a configurarlas para asociar sus WorkMail usuarios de Amazon al Centro de Identidad de IAM.

Los usuarios y grupos sincronizados con su directorio del centro de identidad de IAM están disponibles para asignarlos a su aplicación de Amazon WorkMail. Para obtener más información sobre la gestión de usuarios y grupos del IAM Identity Center, consulte Comenzar con las tareas habituales en el IAM Identity Center. .

Para asignar usuarios y grupos del Centro de identidad de IAM a Amazon WorkMail, sigue estos pasos.

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, selecciona Identity Center.

   Aparece la página de configuración del IAM Identity Center.
3. Elija Asignar usuarios y grupos.

   Puede añadir y asignar nuevos usuarios o asignar usuarios y grupos existentes.

   - Asignar usuarios: puede asignar usuarios individuales del Centro de Identidad de IAM a Amazon WorkMail. Puede crear un nuevo usuario del Centro de Identidad de IAM o buscar un usuario existente.
   - Asignar grupos: también puedes asignar un grupo del centro de identidad de IAM a Amazon WorkMail. A continuación, todos los miembros del grupo se asignarán a Amazon WorkMail.

> **Note**
>
> Todos los nuevos usuarios del Centro de Identidad de IAM están habilitados de forma predeterminada en el Centro de Identidad de IAM. Para conceder acceso a Amazon WorkMail, debes configurar su contraseña en el Centro de Identidad de IAM y asignarla a Amazon WorkMail. Para obtener más información, consulte Añadir usuarios al directorio de su centro de identidad.

Asociación de usuarios de Amazon con WorkMail usuarios del Centro de Identidad de IAM

Cuando un usuario inicia sesión en el cliente WorkMail web de Amazon con sus credenciales de usuario del IAM Identity Center, el cliente abrirá el buzón del WorkMail usuario de Amazon asociado. Si ningún usuario de la WorkMail organización está asociado al usuario del Centro de Identidad de IAM, WorkMail se creará una asociación entre el usuario del Centro de Identidad de IAM que inicie sesión y el WorkMail usuario que tenga el mismo nombre de usuario, si existe dicho usuario. WorkMail De lo contrario, el cliente mostrará un mensaje de error al usuario.

> **Note**
>
> Se recomienda utilizar el mismo nombre de usuario para un usuario en Amazon WorkMail y en el Centro de Identidad de IAM, ya que WorkMail se creará la asociación automáticamente cuando el usuario inicie sesión por primera vez en el cliente WorkMail web de Amazon con sus credenciales de usuario del Centro de Identidad de IAM. Si los nombres de usuario son diferentes, usted es responsable de crear la asociación.

Para asociar usuarios, sigue estos pasos.

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.
2. En el panel de navegación, selecciona Identity Center.

Aparece la página de configuración del IAM Identity Center.

3. Seleccione Asociar usuarios.
4. En Selecciona un WorkMail usuario, selecciona el WorkMail usuario de Amazon que deseas asociar.
5. En Introduzca el ID de usuario del Centro de Identidad de IAM, introduzca el ID del usuario del Centro de Identidad de IAM que desee asociar. Puede copiar el ID de la pestaña Usuarios asignados de la página del Centro de identidades.

   > **Note**
   >
   > El usuario del Centro de Identidad de IAM debe estar autorizado para acceder a la WorkMail aplicación Amazon.

6. Elija Asociar usuarios.

   Una vez que la asociación se haya realizado correctamente, el WorkMail usuario de Amazon puede iniciar sesión en Amazon WorkMail con las credenciales del MFA IAM Identity Center.

> **Note**
>
> También puede asociar los usuarios de Amazon con WorkMail los usuarios del Centro de Identidad de IAM al editar los detalles de los usuarios WorkMail de Amazon. Para obtener más información, consulte Modificación de los detalles de los usuarios.

Modo de autenticación

Puede utilizar el modo de autenticación para permitir a los usuarios iniciar sesión con sus credenciales del WorkMail directorio de Amazon o sus credenciales del IAM Identity Center o restringir el inicio de sesión solo a las credenciales del IAM Identity Center.

Hay dos modos de autenticación disponibles en Amazon WorkMail.

> **Note**
>
> La elección del modo de autenticación depende de los requisitos de seguridad de la organización y de las preferencias de experiencia del usuario. Se recomienda utilizar solo

el modo IAM Identity Center, ya que proporciona una seguridad mejorada al aplicar las credenciales del IAM Identity Center y el MFA. Sin embargo, antes de cambiar del modo Amazon WorkMail Directory y IAM Identity Center, asegúrese de probar el proceso de MFA con todos sus usuarios para garantizar una transición fluida y evitar cualquier impacto en el acceso de los clientes de correo electrónico existentes.

- Amazon WorkMail Directory y el centro de identidad de IAM (recomendado para las pruebas): esta es la opción predeterminada para probar las asociaciones del centro de identidad de IAM antes de cambiar al modo de producción. El modo de prueba permite a los usuarios iniciar sesión en el cliente WorkMail web de Amazon con las credenciales del WorkMail directorio de Amazon y del IAM Identity Center. Al compartir la URL de la aplicación WorkMail web de Amazon desde la configuración de la organización, el usuario puede iniciar sesión con sus credenciales del WorkMail directorio de Amazon. Al compartir la URL habilitada para MFA desde la configuración del Centro de identidad de IAM, el usuario puede iniciar sesión con sus credenciales de IAM.
- Solo IAM Identity Center (recomendado para producción): este modo de autenticación solo le permite iniciar sesión en el buzón de correo del WorkMail cliente de Amazon con las credenciales del IAM Identity Center. Para WorkMail los usuarios actuales de Amazon, las credenciales del WorkMail directorio de Amazon ya no son válidas ni para la aplicación WorkMail web de Amazon ni para ningún cliente de correo electrónico existente. Puedes solicitar un token de acceso personal para acceder al buzón mediante cualquier cliente de correo electrónico. Para evitar perder el acceso a los buzones, asegúrese de que la MFA esté habilitada para todos los usuarios de Amazon WorkMail .

Para activar el modo de autenticación, sigue estos pasos.

1. En la página de configuración del Identity Center, seleccione la pestaña Modo de autenticación.
2. Elija Edit (Edición de).

   Aparece la página Editar el modo de autenticación.
3. Seleccione una de estas opciones:

   - Solo IAM Identity Center
   - Amazon WorkMail Directory y centro de identidad de IAM
4. Seleccione Save.

Configuración de los tokens de acceso personal

Puedes habilitar el token de acceso personal para que WorkMail los usuarios de Amazon accedan a sus buzones mediante clientes de correo electrónico móviles y de escritorio. Una vez activado el Centro de identidad de IAM, el estado del token de acceso personal se establece de forma predeterminada como activo y es válido durante 365 días. Tras activar el Centro de identidad de IAM, las credenciales existentes de sus usuarios dejarán de ser válidas para iniciar sesión en sus clientes de correo electrónico. Sus usuarios pueden generar el token de acceso personal desde la aplicación WorkMail web de Amazon y usarlo para iniciar sesión en cualquier cliente de correo electrónico. Puede editar la caducidad del token de acceso personal y, cuando caduque, su usuario podrá generar uno nuevo.

> **Note**
>
> - Tu usuario solo podrá ver y copiar tu token de acceso personal una vez cuando lo crees en Amazon WorkMail. Si pierdes tu token de acceso personal, tendrás que generar uno nuevo por motivos de seguridad.
> - Amazon WorkMail solo permite los tokens de acceso personal para el acceso a los buzones cuando el WorkMail usuario de Amazon está asociado a un usuario del Centro de Identidad de IAM que esté autorizado a acceder a la WorkMail aplicación de Amazon.

Las configuraciones de los tokens de acceso personal se enumeran a continuación:

- Activo: cuando el estado del token de acceso personal se establece en Activo, el usuario puede generar un token de acceso personal desde Amazon WorkMail y usarlo para iniciar sesión en cualquier cliente de correo electrónico durante la vigencia del token.
- Inactivo: si el estado del token de acceso personal se establece en Inactivo, el usuario no podrá generar ni utilizar los tokens de acceso personal para acceder a los buzones de correo.
- Duración del token: de forma predeterminada, el token de acceso personal es válido durante 365 días. Tiene la opción de cambiar la duración del token de acceso personal. Si dejas en blanco la opción de vida útil, el token tendrá una vida útil indefinida y nunca caducará.

Para configurar los tokens de acceso personal, sigue estos pasos.

1. En la página de configuración del Identity Center, seleccione la pestaña de configuración del token de acceso personal.
2. Elija Edit (Edición de).

   Aparece la página Editar la configuración del token personal.
3. En el estado del token, deslice el botón Activo para habilitar el token de acceso personal.
4. En el cuadro de texto Duración del token (en días), introduzca el número de días que se puede activar el token de acceso personal.
5. Seleccione Save.

Desactivar el Centro de identidad de IAM

Puede deshabilitar el Centro de identidades de IAM desde la WorkMail consola de Amazon. Una vez desactivada, no podrá acceder al buzón con las credenciales del Centro de Identidad de IAM ni con los tokens de acceso personal. Se recomienda restablecer todas las contraseñas de los usuarios y los WorkMail usuarios de Amazon volverán a utilizar las credenciales de Amazon WorkMail Directory.

> **Note**
>
> Comprueba lo siguiente:
>
> - Tras desactivar el Centro de identidades de IAM, los usuarios y grupos de Amazon WorkMail y del Centro de identidades de IAM permanecerán inalterados.
> - Las asociaciones de usuarios existentes seguirán existiendo.
> - La autenticación volverá a ser gestionada por el WorkMail directorio de Amazon, en lugar de por el Centro de identidades de IAM.

Para deshabilitar el Centro de identidad de IAM, sigue estos pasos.

1. En la página de configuración del Identity Center, seleccione Desactivar.

   Aparece la página Desactivar el centro de identidad de IAM.
2. Elija Confirmar.

Uso de dispositivos móviles

En los temas de esta sección se explica cómo gestionar los dispositivos móviles conectados a Amazon WorkMail.

Temas

Modificación de la política de dispositivos móviles de la organización

Puedes editar la política de dispositivos móviles de tu organización para cambiar la forma en que los dispositivos móviles interactúan con Amazon WorkMail.

Para editar la política de dispositivos móviles de la organización

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la Región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccionar una región y elija una región. Para obtener más información, consulte Nombre de región y puntos de conexión en Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Mobile Policies y, a continuación, en la pantalla Default mobile policy, elija Edit.
4. Actualice cualquiera de los siguientes parámetros cuanto sea necesario:

   a. Exigir cifrado en dispositivo: cifre los datos de correo electrónico en el dispositivo móvil.
   b. Exigir cifrado en tarjeta de almacenamiento: cifre los datos de correo electrónico en la tarjeta extraíble del dispositivo móvil.

c. Contraseña obligatoria: solicite una contraseña para desbloquear un dispositivo móvil.

d. Permitir el uso de contraseña simple: utilice el PIN del dispositivo como contraseña.

e. Longitud mínima de la contraseña: establezca el número de caracteres necesario para una contraseña válida.

f. Exigir contraseña alfanumérica: exija que las contraseñas consistan de letras y números.

g. Número de intentos fallidos permitidos: especifique el número de intentos fallidos de desbloqueo del dispositivo que se permiten antes de que se borre el dispositivo del usuario. Todos los datos, incluidos los archivos personales, se eliminarán cuando se borre el dispositivo.

h. Vencimiento de contraseña: especifique el número de días antes del vencimiento de una contraseña y cuándo debe cambiarse.

i. Habilitar el bloqueo de pantalla: especifique el número de segundos que deben transcurrir sin entradas del usuario para bloquear la pantalla del usuario.

j. Aplicar el historial de contraseñas: especifique el número de contraseñas que pueden escribirse antes de repetir la misma contraseña.

5. Seleccione Guardar.

Administración de dispositivos móviles

En los temas de esta sección se explica cómo eliminar datos de dispositivos móviles de forma remota, eliminar dispositivos de su organización y ver detalles de dispositivos. Para obtener información sobre cómo modificar la política de dispositivos móviles de su organización, consulte Modificación de la política de dispositivos móviles de la organización.

Temas

Eliminación de datos de dispositivos móviles de forma remota

Los pasos de esta sección explican cómo eliminar datos de dispositivos móviles de forma remota. Recuerde lo siguiente:

- Los dispositivos deben estar en línea y conectados a Amazon WorkMail. Si alguien desconectase un dispositivo, la operación de eliminación de datos se reanuda apenas el usuario vuelva a conectarlo.
- Las operaciones de eliminación de datos pueden tardar cinco minutos en propagarse.

> **Important**
>
> Para la mayoría de los dispositivos móviles, un borrado remoto restablece el dispositivo en valores predeterminados de fábrica. Todos los datos, incluidos los archivos personales, se pueden quitar al realizar este procedimiento.

Para borrar de forma remota el dispositivo móvil de un usuario

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la Región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccionar una región y elija una región. Para obtener más información, consulte Nombre de región y puntos de conexión en Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Usuarios, y en la lista de usuarios, seleccione el nombre del usuario de cuyo dispositivo necesita eliminar datos.
4. Elija la pestaña Dispositivos móviles.
5. En la lista de dispositivos, seleccione el botón situado junto al dispositivo y, a continuación, elija Eliminar datos.
6. Compruebe el estado en la vista de resumen para ver si se ha solicitado la eliminación de datos.
7. Después de eliminar los datos del dispositivo, elimine el dispositivo de la lista de dispositivos. Los pasos indicados en la siguiente sección explican cómo hacerlo.

> **Important**
>
> Para devolver un dispositivo con datos eliminados a la lista de dispositivos de un usuario, asegúrese de eliminarlo primero de la lista de dispositivos. De lo contrario, el sistema volverá a eliminar los datos del dispositivo.

Eliminación de dispositivos móviles de los usuarios de la lista de dispositivos

Si alguien dejase de utilizar un dispositivo móvil específico, o usted ha eliminado los datos del dispositivo de forma remota, puede eliminar el dispositivo de la lista de dispositivos. Cuando el usuario vuelve a configurar el dispositivo, se muestra en la lista.

Para quitar los dispositivos móviles de un usuario de la lista de dispositivos

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambie la Región de AWS. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Usuarios y luego seleccione el nombre del usuario.
4. Elija la pestaña Dispositivos móviles.
5. En la lista de dispositivos, seleccione el botón situado junto al dispositivo y luego Eliminar.

Visualización de los detalles de los dispositivos móviles

Puede ver los detalles del dispositivo móvil de un usuario.

> **Note**
>
> Algunos dispositivos no envían todos sus detalles al servidor. Es posible que no vea todos los detalles disponibles del dispositivo.

Para ver los detalles del dispositivo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   De ser necesario, cambie la región. En la barra de navegación, seleccione la región adecuada a sus necesidades. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Usuarios y luego la pestaña Dispositivos móviles.
4. En la lista de dispositivos, seleccione el ID del dispositivo del cual desea ver detalles.

   En la siguiente tabla se enumeran los códigos de estado de un dispositivo.

Estado	Descripción
`PROVISIONING_REQUIRED`	Un usuario o administrador ha solicitado que se aprovisione el dispositivo para su uso con Amazon WorkMail. Los dispositivos también se configuran en este estado si la política actual de ese dispositivo se modifica en la WorkMail consola de Amazon.
`PROVISIONING_SUCCEEDED`	El dispositivo se ha preparado correctam ente. El dispositivo ha aplicado la política indicada.
`WIPE_REQUIRED`	Un administrador solicitó que se eliminara el contenido de la WorkMail consola de Amazon.

Estado	Descripción
`WIPE_SUCCEEDED`	Los datos del dispositivo se han eliminado correctamente.

Administración de reglas de acceso de dispositivos móviles

Las reglas de acceso a dispositivos móviles de Amazon WorkMail permiten a los administradores controlar el acceso a los buzones de determinados tipos de dispositivos móviles. De forma predeterminada, cada WorkMail organización de Amazon usa una regla que otorga acceso al buzón de correo a cualquier dispositivo, independientemente del tipo, modelo, sistema operativo o agente de usuario. Puede editar o sustituir esa regla predeterminada por una propia. También puede añadir, modificar y eliminar reglas.

> **Warning**
>
> Si eliminas todas las reglas de acceso a dispositivos móviles de una organización, Amazon WorkMail bloquea el acceso a todos los dispositivos móviles.

Puede crear reglas que permitan o denieguen el acceso en función de las siguientes propiedades del dispositivo:

- Tipo de dispositivo: “iPhone”, “iPad” o “Android”.
- Modelo de dispositivo: «iPhone 10C1", «iPad 5C1" o «X» HTCOne
- Sistema operativo del dispositivo: “iOS 12.3.1 16F203” o “Android 8.1.0”.
- Agente de usuario del dispositivo: “iOS/14.2 (18B92) exchangesyncd/1.0” o “Android-Mail/7.7.16.163886392.release”.

Para ver las propiedades del dispositivo en la consola de administración, consulte Visualización de los detalles del dispositivo móvil. AWS

> **Note**
>
> Es posible que algunos dispositivos y clientes no informen de las propiedades de todos los campos. Para obtener información sobre cómo solucionar esos casos, consulte Dealing with empty fields

> **Important**
>
> Las reglas de acceso a dispositivos WorkMail móviles de Amazon solo se aplican a los dispositivos que utilizan el ActiveSync protocolo Microsoft Exchange. Los clientes móviles que utilicen un protocolo diferente, como IMAP, no informan de las propiedades del dispositivo que se enumeran aquí, por lo que estas reglas no se aplican.
> Si necesita restringir el acceso de dispositivos que utilicen otros protocolos, puede crear reglas de control de acceso. Para obtener más información sobre las mismas, consulte Uso de reglas de control de acceso. Por ejemplo, puede restringir el acceso a otros protocolos y al correo web solo a un rango de direcciones IP corporativas, pero permitir que Microsoft acceda a otro lugar y, luego, usar las reglas ActiveSync de acceso a dispositivos móviles para limitar aún más los tipos y versiones de los clientes permitidos.

Temas

Cómo funcionan las reglas de acceso de dispositivos móviles

Las reglas de acceso a dispositivos móviles solo se aplican a los dispositivos que utilizan el ActiveSync protocolo Microsoft Exchange. Cada regla tiene un conjunto de condiciones que especifican cuándo se aplica la regla, además de un efecto de acceso de `ALLOW` o `DENY` para el dispositivo. Una regla se aplica a una solicitud de acceso solo si todas las condiciones de la regla coinciden con las propiedades del dispositivo móvil del usuario. Las reglas sin condiciones se aplican a todas las solicitudes. Cada condición utiliza una coincidencia de prefijo que no distingue entre mayúsculas y minúsculas con las propiedades notificadas del dispositivo.

Amazon WorkMail evalúa las reglas de la siguiente manera:

- Si cualquier regla `DENY` coincide con una propiedad del dispositivo, la política bloquea el dispositivo. Las reglas `DENY` tienen prioridad sobre las reglas `ALLOW`.
- Si al menos una regla `ALLOW` coincide y ninguna regla `DENY` coincide, la política permite el dispositivo.
- Si no se aplica ninguna regla, se bloquea el dispositivo.

> **Important**
>
> Los dispositivos móviles notifican las propiedades que las reglas utilizan para funcionar. Los dispositivos informan de sus propiedades durante el proceso de aprovisionamiento de ActiveSync dispositivos de Microsoft. Amazon WorkMail no puede verificar de forma independiente si los clientes móviles informan de forma correcta o con up-to-date información correcta.

Uso de las reglas de acceso de dispositivos móviles

Puede usar APIs o la interfaz de línea de comandos (CLI) de AWS para crear y administrar reglas de acceso para dispositivos móviles. Para obtener más información al respecto AWS CLI, consulte la Guía del usuario de la interfaz de línea de comandos de AWS.

> **Important**
>
> Cuando cambias una regla de acceso para una WorkMail organización de Amazon, los dispositivos afectados pueden tardar cinco minutos en seguir la regla actualizada y, durante ese tiempo, los dispositivos pueden mostrar un comportamiento incoherente. Sin embargo, verá de inmediato un comportamiento correcto al probar las reglas. Para obtener más información, consulte Testing mobile device access rules.

Listado de reglas de acceso de dispositivos móviles

El siguiente ejemplo muestra cómo obtener una lista de reglas de acceso de dispositivos móviles.

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Creación de reglas de acceso de dispositivos móviles

En el siguiente ejemplo se crea una regla que bloquea el acceso a los buzones de correo de cualquier dispositivo Android.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

En el siguiente ejemplo se crea una regla que permite solo una versión específica de iOS. Asegúrese de eliminar la regla predeterminada `ALLOW-all`.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

Actualización de reglas de acceso de dispositivos móviles

En el siguiente ejemplo se actualiza una regla de dispositivo añadiendo un identificador.

```
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"
```

Eliminación de una regla de acceso de dispositivos móviles

En el siguiente ejemplo se elimina la regla de acceso de dispositivos móviles con el identificador dado.

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

Prueba de reglas de acceso de dispositivos móviles

Para probar las reglas de acceso, puedes usar la GetMobileDeviceAccessEffectAPI o el comando get-mobile-device-access -effect del AWS CLI . Para obtener más información sobre el AWS CLI, consulte la Guía del usuario de la interfaz de línea de AWS comandos.

Al realizar la prueba, se pasan las propiedades de un dispositivo móvil simulado y la API o CLI devuelven el efecto de acceso —`ALLOW` o `DENY`— que recibiría un dispositivo móvil real con esas

propiedades. Por ejemplo, este comando comprueba si un iPhone con iOS 14.2 y la aplicación de correo predeterminada pueden acceder a un buzón de correo.

```
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"
```

Tratamiento de campos vacíos

Es posible que algunos dispositivos móviles o clientes no proporcionen información para uno o más campos, dejando los valores vacíos. Las reglas pueden cotejarse frente a estos dispositivos utilizando el valor especial `$NONE` en una condición. Por ejemplo, una regla con `DeviceTypes=["iphone", "ipad", "$NONE"]` coincidirá con los dispositivos que notifiquen un tipo de dispositivo `"iphone"` o `"ipad"`, o que no notifiquen en absoluto un tipo de dispositivo.

Las condiciones negativas como `NotDeviceTypes` o `NotDeviceUserAgents` no coincidirán con estos valores vacíos. Por ejemplo, una regla con `NotDeviceTypes=["android"]` coincidirá con los dispositivos que notifiquen un tipo de dispositivo distinto de `"android"`. Sin embargo, la regla no coincidirá con los dispositivos que no notifiquen en absoluto un tipo de dispositivo.

Administración de anulaciones de acceso de dispositivos móviles

Las anulaciones de acceso de dispositivos móviles se utilizan para anular los resultados de las reglas de acceso de dispositivos móviles. Las anulaciones se aplican a usuarios y dispositivos específicos, e invierte la regla de acceso predeterminada. También puede utilizar anulaciones para crear excepciones puntuales a las reglas de acceso y permitir o denegar pares específicos de usuarios y dispositivos. Además, puede utilizar anulaciones con una regla de acceso de dispositivos móviles `DefaultDenyAll`. Eso aplaza las decisiones de acceso a una solución de administración de dispositivos móviles (MDM) de terceros. Para obtener más información, consulte Administración de las anulaciones y Integración con soluciones de administración de dispositivos móviles.

Temas

- Cómo funcionan las anulaciones de acceso de dispositivos móviles
- Administración de las anulaciones

Cómo funcionan las anulaciones de acceso de dispositivos móviles

Usted crea anulaciones de acceso de dispositivos móviles para un par usuario-dispositivo específico. La anulación invierte el resultado de acceso predeterminado al evaluar las reglas de acceso de dispositivos móviles para un usuario y dispositivo determinados. Por ejemplo, si una regla de acceso normalmente deniega el acceso, una anulación de acceso permite a ese usuario y dispositivo sincronizar su correo electrónico. Por el contrario, si una regla de acceso normalmente permite el acceso, puede crear una anulación que impida que el usuario y el dispositivo sincronicen su correo. Cuando eliminas la anulación de acceso a un dispositivo móvil, Amazon WorkMail vuelve a respetar el resultado de las normas de acceso a dispositivos móviles actuales a la hora de decidir si concede el acceso a ese usuario y dispositivo.

> **Important**
>
> Cuando cambias la anulación de acceso de un dispositivo móvil para una WorkMail organización de Amazon, los dispositivos afectados pueden tardar cinco minutos en seguir la anulación actualizada.

Administración de las anulaciones

Las anulaciones de acceso de dispositivos móviles pueden crearse, actualizarse o eliminarse mediante la API o la AWS Command Line Interface. Para obtener más información al respecto AWS CLI, consulte la Guía del usuario de la interfaz de línea de comandos de AWS.

Para encontrar el ID del dispositivo, utilice la AWS Management Console. Para obtener más información, consulte Visualización de detalles de dispositivos móviles.

Listado de anulaciones de acceso de dispositivos móviles

En este ejemplo, se muestra cómo enumerar todas las anulaciones de acceso a dispositivos móviles de una WorkMail organización de Amazon específica.

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Creación y actualización de anulaciones de acceso de dispositivos móviles

Esto creará una anulación del acceso al dispositivo móvil para denegar el acceso a la WorkMail organización, el usuario y el ID de dispositivo de Amazon especificados.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect DENY
```

Se puede modificar una anulación de acceso de dispositivos móviles existente para que tenga un efecto diferente. Esto actualiza la anulación de acceso de dispositivos móviles creada anteriormente para permitir el acceso en vez de denegarlo.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect ALLOW
```

Eliminación de anulaciones de acceso de dispositivos móviles

Esto eliminará la anulación de acceso al dispositivo móvil para la WorkMail organización, el usuario y el ID de dispositivo de Amazon especificados.

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0
```

Integración con soluciones de administración de dispositivos móviles

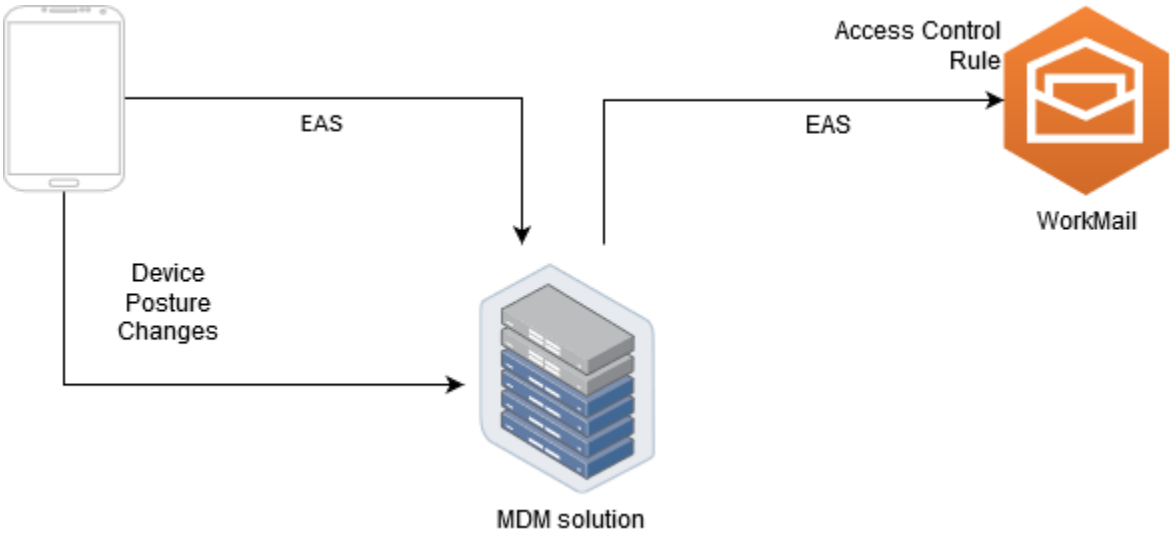
Amazon WorkMail admite algunas funciones básicas de administración de dispositivos móviles mediante políticas de dispositivos móviles y reglas de acceso a dispositivos móviles. Sin embargo, esas funciones solo pueden interactuar con los dispositivos móviles a través del protocolo Microsoft Exchange ActiveSync (EAS), por lo que tienen una capacidad limitada de introspección y aplicación de la postura de seguridad del dispositivo. Los administradores que necesiten un mayor control de la seguridad y el cumplimiento de los dispositivos pueden utilizar una solución de administración de dispositivos móviles (MDM) de terceros.

Información general sobre soluciones de administración de dispositivos móviles

Puede configurar su solución MDM en dos modos, proxy o directo. Consulte la documentación de MDM para informarse de los modos que su solución admite.

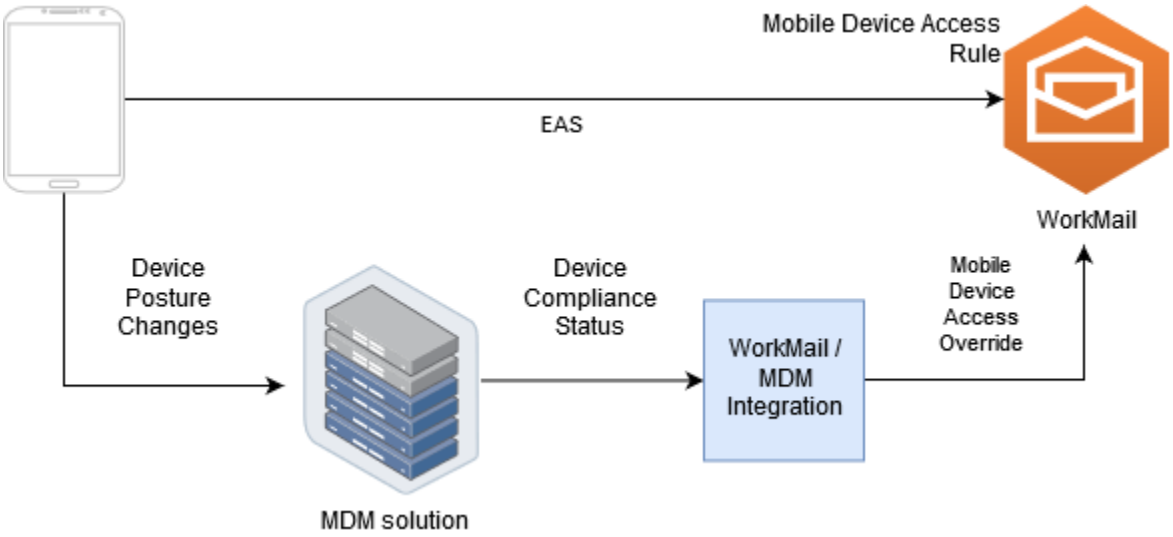
En el modo proxy, los dispositivos móviles utilizan el protocolo Exchange Active Sync (EAS) a través de su solución MDM para acceder a Amazon WorkMail. La solución MDM utiliza la postura del dispositivo para permitir o denegar el acceso a los WorkMail datos de Amazon. WorkMail Por parte de Amazon, utilice una regla de control de acceso que permita el acceso de EAS únicamente desde la dirección o direcciones IP de la solución MDM. Para obtener más información, consulte Uso de reglas de control de acceso.

En la siguiente imagen se muestra una configuración típica en modo proxy.



En el modo directo, los dispositivos móviles utilizan EAS para acceder WorkMail directamente a Amazon. Su solución MDM recibe los cambios de postura del dispositivo y evalúa continuamente si cada dispositivo cumple esos requisitos. Cuando la solución MDM detecta un cambio de postura, como que un dispositivo no cumple los requisitos, puede tomar varias medidas y suele emitir notificaciones o eventos. Un WorkMail administrador de Amazon puede configurar un sistema para escuchar estos eventos de estado de conformidad y crear automáticamente anulaciones de acceso a los dispositivos móviles que permitan o denieguen el acceso a los dispositivos cuando entran o no cumplen con los requisitos de los dispositivos MDM.

En la siguiente imagen se muestra una configuración típica en modo directo.



Configurar una WorkMail organización para que se integre con una solución de MDM de terceros en modo directo

Para integrarse con una solución de administración de dispositivos móviles (MDM) de terceros en modo directo, debe cumplir estos requisitos:

- Cree reglas de control de acceso que restrinjan el acceso a los dispositivos de los usuarios únicamente al ActiveSync protocolo.
- Cree una regla de acceso a dispositivos móviles deny-to-all «» predeterminada para garantizar que se deniegue de forma predeterminada a todos los dispositivos móviles desconocidos o no gestionados.
- Adopte una solución de administración de dispositivos móviles que emita notificaciones o eventos personalizados cuando un dispositivo cambie de postura de seguridad, es decir, al entrar o salir de la conformidad.
- Crea un componente de software personalizado para escuchar esas notificaciones y llama al Amazon WorkMail SDK para crear anulaciones de acceso desde dispositivos móviles.

Estos componentes garantizan que todos los dispositivos de los usuarios cumplan con sus requisitos de conformidad con la MDM antes de que se les permita acceder a sus WorkMail buzones de Amazon.

Utilice las reglas de control de acceso para restringir el acceso de los dispositivos móviles a ActiveSync

Debe asegurarse de que todos los dispositivos utilicen únicamente el ActiveSync protocolo y, para ello, puede utilizar las reglas de control de acceso. Por ejemplo, puede conceder acceso a otros protocolos de correo únicamente desde un rango interno de direcciones IP corporativas y, a continuación, permitir únicamente el acceso ActiveSync al correo electrónico desde fuera del firewall corporativo. Debe hacerlo porque solo ActiveSync le permite identificar los dispositivos mediante un ID de dispositivo. No puede utilizar protocolos como el Protocolo de Acceso a Mensajes de Internet (IMAP) o Exchange Web Services. Para obtener más información, consulte Uso de reglas de control de acceso.

Creación de una regla de acceso predeterminada “denegar a todos”

Para aplazar todas las decisiones de acceso de dispositivos móviles a la solución de administración de dispositivos móviles de terceros, cree una regla de acceso que deniegue automáticamente el acceso a todos los dispositivos a menos que se anule por usuario o por dispositivo. Para obtener más información, consulta Administración de reglas de acceso de dispositivos móviles.

En este ejemplo se muestra una regla “denegar a todos”.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

Reacción a cambios de postura de dispositivos y creación de anulaciones de acceso de dispositivos móviles

Debe configurar su solución MDM para que envíe notificaciones sobre los cambios de postura de un dispositivo. Estas notificaciones deben ser consumidas por un componente que pueda usar el Amazon WorkMail SDK para crear o actualizar las anulaciones de acceso de los dispositivos móviles. De forma predeterminada, Amazon WorkMail deniega el acceso a los dispositivos no gestionados o recién aprovisionados debido a la regla predeterminada de «denegar el acceso a todos los dispositivos móviles» que se muestra anteriormente en este tema. Cuando la solución MDM determine que el dispositivo cumple todos los requisitos y emita una notificación indicando que el dispositivo es conforme, este componente puede reaccionar a esta notificación creando una anulación de acceso de dispositivos móviles con un efecto de `ALLOW` para el usuario y el dispositivo especificados. Si posteriormente el dispositivo deja de ser conforme, la solución de administración de dispositivos móviles emite otra notificación, y la anulación de acceso puede eliminarse o modificarse para denegar el acceso de ese dispositivo. Para obtener más información, consulte Administración de anulaciones de acceso de dispositivos móviles.

Para ver un ejemplo de Amazon WorkMail integrado con MDM, consulta este AWS ejemplo de aplicación.

Uso de los permisos del buzón de correo

Puedes usar los permisos de buzón en Amazon WorkMail para conceder a los usuarios y grupos el derecho a trabajar en los buzones de otros usuarios. Los permisos de buzón de correo se aplican a todo un buzón de correo. Permiten a múltiples usuarios el acceso al mismo buzón de correo sin compartir las credenciales de dicho buzón. Los usuarios con permisos del buzón pueden leer y modificar los datos de este y enviar correo electrónico desde el buzón compartido.

> **Note**
>
> Los usuarios con permisos para un buzón de correo perteneciente a un usuario oculto de la lista global de direcciones pueden seguir accediendo al buzón de correo del usuario oculto.

En la siguiente lista, se enumeran los permisos que puede conceder:

- Acceso total: habilita el acceso total de lectura y escritura al buzón de correo, incluyendo los permisos para modificar permisos a nivel de carpeta.

  > **Note**
  >
  > Esta opción solo está disponible para usuarios. A los grupos no se les pueden conceder derechos de acceso total.

- Enviar en nombre de: habilita a un usuario o grupo a enviar correo electrónico en nombre de otro usuario. El propietario del buzón aparece en el encabezado From: (De:) y la persona que envía el mensaje, en el encabezado Sender: (Remitente:).
- Enviar como: habilita a un usuario o grupo a enviar correo electrónico como propietario del buzón de correo, sin mostrar el remitente real del mensaje. El propietario del buzón aparece en los encabezados From: (De:) y Sender: (Remitente:).
- Ninguno: impide que un usuario o grupo envíe correos electrónicos.

> **Note**
>
> Si se conceden permisos del buzón de correo a un grupo, estos permisos se extienden a todos los miembros de dicho grupo, incluidos los miembros de los grupos anidados.

Cuando concedes permisos a los buzones de correo, el WorkMail AutoDiscover servicio de Amazon actualiza automáticamente el acceso a esos buzones para los usuarios o grupos que has añadido.

En el caso del cliente de Microsoft Outlook de Windows, los usuarios que tengan acceso completo podrán obtener acceso automáticamente a los buzones de correo compartidos. Debe esperar hasta 60 minutos para que los cambios se propaguen y, a continuación, reinicie Microsoft Outlook.

En la aplicación WorkMail web Amazon y en otros clientes de correo electrónico, los usuarios con permisos de acceso total pueden abrir manualmente los buzones compartidos. Los buzones de correo abiertos se mantendrán así, incluso entre sesiones, a menos que el usuario los cierre.

Temas

Información acerca de los permisos de buzones de correo y carpetas

Los permisos de buzón de correo se aplican a todas las carpetas de un buzón de correo. Estos permisos solo los puede habilitar el titular de la AWS cuenta o un usuario de IAM autorizado a llamar a la API de WorkMail administración de Amazon. Para configurar y cambiar los permisos de los buzones de correo o de los grupos en su conjunto, usa la API de Amazon AWS Management Console o la WorkMail API. Puede administrar hasta 100 buzones de correo y permisos de grupo desde la consola. Para gestionar los permisos de más usuarios y grupos, usa la WorkMail API de Amazon.

Los permisos de carpeta se aplican a una única carpeta. Los usuarios finales pueden establecer los permisos de las carpetas mediante un cliente de correo electrónico o mediante la aplicación WorkMail web Amazon. Para obtener más información sobre el uso de la aplicación WorkMail web de Amazon para compartir carpetas, consulte Compartir carpetas y permisos de carpetas en la Guía del WorkMail usuario de Amazon.

Administración de permisos del buzón de correo para usuarios

Puedes usar la WorkMail consola de Amazon para gestionar los permisos de los buzones de correo de los usuarios y de los grupos. En las secciones siguientes se explica la forma de administrar los

permisos para usuarios. Para obtener información sobre cómo administrar permisos para grupos, consulte Administración de permisos del buzón de correo para grupos.

Temas

Adición de permisos

Al añadir permisos, concede a un usuario el derecho a realizar una o varias tareas en el buzón de correo de otro usuario. Por ejemplo, supongamos que el empleado A necesita enviar mensajes en nombre de su supervisor, el empleado B. Para conceder ese permiso, vaya a la configuración del buzón de correo del empleado B y conceda al empleado A permiso para realizar la tarea solicitada.

Para añadir permisos al buzón de correo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   De ser necesario, cambie la región. En la barra de navegación, elija la región que se ajuste a sus necesidades. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, seleccione el nombre de la organización para la que desea administrar los permisos.
3. En el panel de navegación, elija Usuarios y, a continuación, seleccione el nombre del usuario para el que desea administrar los permisos.
4. Seleccione la pestaña Permisos y, a continuación, seleccione Añadir permisos.

   Aparece el cuadro de diálogo Añadir permisos.
5. Abra la lista Añadir nuevos permisos y seleccione el usuario o grupo que necesite acceso al buzón de correo.
6. En Permisos de buzón de correo y Permisos de envío, elija las opciones deseadas.
7. Elija Añadir.

Los nuevos permisos pueden tardar hasta cinco minutos en propagarse a los usuarios.

Edición de permisos de buzón de correo para usuarios

Al editar permisos del buzón de correo de un usuario, se modifica el acceso que otras personas tienen al buzón de correo de ese usuario. La edición de permisos de buzón de correo no cambia el acceso para el usuario original del buzón.

Para editar permisos de buzón de correo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   De ser necesario, cambie la región. En la barra de navegación, elija la región que se ajuste a sus necesidades. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, seleccione el nombre de la organización para la que desea administrar los permisos.
3. En el panel de navegación, elija Usuarios y, a continuación, seleccione el nombre del usuario cuyos permisos desea editar.
4. Elija la pestaña Permisos.

   Aparece una lista de los usuarios y grupos que tienen acceso al buzón de correo.
5. Seleccione el botón de opción situado junto al usuario o grupo que desee modificar y, a continuación, realice una de las siguientes acciones:

   Eliminación de permisos de un usuario

   1. Elija Eliminar.

      Aparece el cuadro de diálogo Eliminar permisos.
   2. En el cuadro de diálogo Eliminar permisos, elija Eliminar.

   Para editar los permisos de un usuario

   1. Elija Editar.

      Aparece el cuadro de diálogo Editar permisos.
   2. Establezca los permisos según sea necesario y, a continuación, elija Guardar.

Para conceder a otro usuario permisos sobre el buzón de correo

1. Elija Añadir permisos.

   Aparece el cuadro de diálogo Añadir permisos.
2. Abra la lista Añadir nuevos permisos y seleccione el usuario al que desee añadirlos.
3. Establezca los permisos según sea necesario y, a continuación, elija Añadir.

Los cambios realizados en los permisos pueden tardar hasta cinco minutos en propagarse a los usuarios.

Administración de permisos del buzón de correo para grupos

Puedes añadir o eliminar permisos de grupo para Amazon WorkMail.

> **Note**
>
> No puede aplicar permisos de Acceso total a un grupo, dado que los grupos no tienen un buzón de correo al que acceder.

Para administrar los permisos de grupo

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la barra situada Región de AWS en la parte superior de la ventana de la consola, abre la lista Selecciona una región y selecciona una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, seleccione el nombre de la organización para la que desea administrar los permisos.
3. En el panel de navegación, elija Grupos y, a continuación, seleccione el nombre del grupo para el que desea establecer permisos.
4. Elija la pestaña Permisos y, a continuación, elija Añadir permisos.

   Aparece el cuadro de diálogo Añadir permisos.

5. Abra la lista Añadir nuevos permisos y seleccione el usuario o grupo al que desee otorgar permisos para el buzón de correo.
6. En Permisos de buzón de correo y Permisos de envío, elija las opciones deseadas.
7. Elija Agregar.

Los cambios realizados en los permisos pueden tardar hasta cinco minutos en propagarse a los usuarios.

Acceso programático a los buzones de correo

Para acceder mediante programación a los WorkMail buzones de Amazon, utilice el protocolo Exchange Web Services (EWS). Con EWS, puede acceder a todos los tipos de elementos de un buzón de correo. Estas son algunas de las bibliotecas de EWS que puede utilizar con Amazon WorkMail:

- Java: API de Java de EWS
- .Net: API gestionada por EWS
- Python: Exchangelib

Amazon WorkMail también admite los protocolos IMAP y SMTP, que puedes usar para enviar y recibir correos electrónicos. Puedes ver los WorkMail protocolos de Amazon URLs compatibles en los WorkMailpuntos de conexión y las cuotas de Amazon.

Cuando se utiliza el protocolo EWS, Amazon WorkMail admite los siguientes métodos de autenticación:

- Autenticación básica: con la autenticación básica, se introduce una dirección de correo electrónico y una contraseña.
- Roles de suplantación: con los roles de suplantación, usted accede a los buzones de correo de los usuarios sin introducir las credenciales del usuario.

Temas

- Administración de roles de suplantación
- Uso de roles de suplantación

Administración de roles de suplantación

Con los roles de suplantación, los administradores configuran el acceso programático a los buzones de correo de los usuarios sin introducir las credenciales del usuario. Los servicios y herramientas pueden asumir un rol de suplantación para realizar acciones en los buzones de correo de los usuarios. La suplantación solo es compatible con el protocolo EWS.

Información general sobre roles de suplantación

Para permitir la suplantación, los administradores deben crear un rol de suplantación con las siguientes propiedades:

- Tipo de rol: elija entre Acceso total o Solo lectura. El tipo de rol limita el tipo de operaciones que puede realizar un rol.
- Reglas: una lista de reglas que definen a qué usuarios puede suplantar el rol de suplantación.

Amazon WorkMail evalúa las normas en función de las siguientes condiciones:

- Si cualquier regla DENY coincide, la política deniega la suplantación. Las reglas DENY tienen prioridad sobre cualquier regla ALLOW.
- Si al menos una regla ALLOW coincide y no coincide ninguna regla DENY, la política permite la suplantación.
- Si no se aplica ninguna regla, la suplantación se deniega.

> **Note**
>
> Para permitir la suplantación de identidad para todos los usuarios de una WorkMail organización de Amazon, crea una regla con el efecto ALLOW y sin condiciones.

> **Warning**
>
> Debe crear reglas para permitir que un rol de suplantación suplante a un usuario. Si no especifica reglas, un rol de suplantación no puede asumir los derechos de acceso de un usuario.

Una vez creado el rol de suplantación, puede utilizarlo para obtener acceso a los buzones de correo de los usuarios. Para obtener más información, consulte Uso de roles de suplantación.

Consideraciones de seguridad

El uso de funciones de suplantación de identidad crea la posibilidad de que surjan problemas de seguridad en su WorkMail organización de Amazon y. Cuenta de AWS Estos son algunos de los posibles problemas a tener en cuenta al crear un rol de suplantación:

- Permisos transitivos: si el usuario A tiene acceso al buzón de correo del usuario B y se permite que un rol de suplantación suplante al usuario A, entonces este rol de suplantación puede suplantar los permisos de acceso del usuario A y acceder al buzón del usuario B.
- Control de acceso: puede utilizar reglas de control de acceso para limitar el acceso del rol de suplantación. Para obtener más información, consulte Uso de reglas de control de acceso.
- Política de IAM: puedes asignar una `AssumeImpersonationRole` acción a una determinada WorkMail organización de Amazon y a una función de suplantación de identidad mediante la condición. `workmail:ImpersonationRoleId` Para ver un ejemplo de política de IAM, consulte Cómo WorkMail funciona Amazon con IAM.

Creación de roles de suplantación

Puedes crear roles de suplantación desde la consola de Amazon WorkMail .

Para crear un rol de suplantación

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   De ser necesario, cambie la región. En la barra de navegación, elija la región que se ajuste a sus necesidades. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, el nombre de la organización.
3. Elija Roles de suplantación y, a continuación, Crear rol.
4. Aparece el cuadro de diálogo Crear rol de suplantación. En Rol, introduzca la siguiente información:

   - Nombre: introduzca un nombre único para el rol de suplantación.
   - (Opcional) Descripción: introduzca una descripción para el rol de suplantación.
   - Tipo de rol: elija Solo lectura o Acceso total.
5. En Reglas, elija Añadir regla.

6. Aparece el cuadro de diálogo Añadir regla. Introduzca la información siguiente:

   - Nombre: introduzca un nombre exclusivo para la regla.
   - (Opcional) Descripción: introduzca una descripción para la regla.
   - En Efecto, elija Permitir o Denegar. Esto permite o deniega el acceso en función de las condiciones que seleccione en el paso siguiente.
   - (Opcional) En Esta regla:, elija Concuerda solicitudes que suplantan a los usuarios seleccionados para incluir usuarios específicos. Elija Concuerda solicitudes que suplantan a usuarios distintos de los usuarios seleccionados para añadir usuarios distintos de los usuarios seleccionados.
7. Seleccione Añadir regla.

   > **Note**
   >
   > Las reglas solo se guardan cuando se guarda el rol correspondiente.

8. Elija Crear rol.

Edición de roles de suplantación

Puedes editar los roles de suplantación desde la consola de Amazon WorkMail .

Para editar un rol de suplantación

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   De ser necesario, cambie la región. En la barra de navegación, elija la región que se ajuste a sus necesidades. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, el nombre de la organización.
3. Elija Roles de suplantación.
4. Seleccione el nombre del rol de suplantación que desee editar y, a continuación, elija Editar.
5. Aparece el cuadro de diálogo Editar rol de suplantación. En Rol, introduzca la siguiente información:

   - Nombre: introduzca un nombre único para el rol de suplantación.
   - (Opcional) Descripción: introduzca una descripción para el rol de suplantación.

- Tipo de rol: para dar al rol de suplantación acceso de solo lectura al buzón de correo de un usuario, elija Solo lectura. Para otorgar al rol de suplantación derechos de lectura y modificación de los elementos del buzón de correo de un usuario, elija Acceso total.

6. En Reglas, seleccione la regla que desee editar y luego Editar.
7. Aparece el cuadro de diálogo Editar regla. Introduzca la información siguiente:

   - Nombre: edite el nombre de la regla.
   - (Opcional) Descripción: actualice la descripción de la regla o introduzca una.
   - En Efecto, elija Permitir a fin de permitir el acceso cuando se cumplan las condiciones establecidas en las reglas. Para denegar el acceso, elija Denegar.
   - (Opcional) En Esta regla:, elija Concuerda solicitudes que suplantan a los usuarios seleccionados para incluir usuarios específicos. Elija Concuerda solicitudes que suplantan a usuarios distintos de los usuarios seleccionados para añadir usuarios distintos de los usuarios seleccionados.
8. Seleccione Guardar.
9. Elija Guardar cambios.

> **Important**
>
> Al modificar una regla de suplantación, los buzones de correo afectados podrían tardar hasta cinco minutos en actualizarse. Durante el proceso de actualización de la regla, es posible que observe un comportamiento incoherente en su buzón de correo. Sin embargo, si pruebas un rol, Amazon WorkMail responde según lo esperado en función de la regla actualizada. Para obtener más información, consulte Prueba de roles de suplantación.

Prueba de roles de suplantación

Puedes probar un rol de suplantación desde la consola de Amazon WorkMail .

Para probar un rol de suplantación

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

De ser necesario, cambie la región. En la barra de navegación, elija la región que se ajuste a sus necesidades. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.

2. En el panel de navegación, elija Organizaciones y, a continuación, el nombre de la organización.
3. Elija Roles de suplantación.
4. Seleccione el rol de suplantación que desee probar.
5. Elija Probar rol.
6. Aparece el cuadro de diálogo Probar rol de suplantación. En Usuario objetivo, seleccione el usuario para el que desea probar el acceso de suplantación.
7. Seleccione Probar.

Eliminación de roles de suplantación

Puedes eliminar un rol de suplantación de identidad de la consola de Amazon WorkMail .

Para eliminar un rol de suplantación

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   De ser necesario, cambie la región. En la barra de navegación, elija la región que se ajuste a sus necesidades. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, el nombre de la organización.
3. Elija Roles de suplantación.
4. Seleccione el nombre del rol de suplantación que desee eliminar.
5. Elija Eliminar.
6. Aparece el cuadro de diálogo Eliminar rol. Para confirmar la eliminación, introduzca el nombre del rol en el cuadro de diálogo y elija Eliminar.

Uso de roles de suplantación

Para acceder a los datos del buzón, usa la acción de la WorkMail API de Amazon`AssumeImpersonationRole`. Para obtener más información sobre Amazon WorkMail APIs, consulta la Referencia de API.

`AssumeImpersonationRole` devuelve un `Token`. Este `Token` debe transmitirse en un plazo de 15 minutos al protocolo EWS a través del encabezado HTTP `Authorization`.

En los siguientes ejemplos se demuestra cómo utilizar los roles de suplantación con el protocolo EWS. Las constantes utilizadas en los ejemplos especifican los siguientes detalles exclusivos de su organización y cuenta:

- *`WORKMAIL_ORGANIZATION_ID`*— ID de WorkMail organización de Amazon
- *`IMPERSONATION_ROLE_ID`*: ID de rol de suplantación
- *`WORKMAIL_EWS_URL`*— El punto final de EWS está disponible en los WorkMail puntos de conexión y cuotas de Amazon
- *`EMAIL_ADDRESS`*: dirección de correo electrónico del buzón de correo del usuario

Example Java: API de Java de 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 gestionada por 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
)
```

Exportación de contenido de buzones de correo

Utilice la acción de StartMailboxExportJobAPI de la referencia de la WorkMail API de Amazon para exportar el contenido del WorkMail buzón de Amazon a un bucket de Amazon Simple Storage Service (Amazon S3). Esta acción exporta todos los mensajes de correo electrónico y elementos de calendario del buzón especificado a un archivo `.zip` en el bucket de Amazon S3, en formato MIME. Otros elementos, como los contactos y las tareas, no se exportan.

El tiempo que tarda en finalizar el trabajo de exportación del buzón de correo depende del tamaño y del número de elementos del buzón. Dado que el trabajo de exportación del buzón de correo tiene lugar en un periodo de tiempo, no representa una instantánea del contenido del buzón en un único momento. Para ver el estado de un trabajo de exportación, usa las acciones DescribeMailboxExportJobo ListMailboxExportJobsAPI de la Amazon WorkMail API Reference.

Cuando se completa un trabajo de exportación de buzones, el `.zip` archivo del bucket de Amazon S3 se cifra con la clave maestra de cliente AWS Key Management Service (CMK AWS KMS) symmetric () que usted proporciona. Como el AWS KMS cifrado está integrado en Amazon S3, los datos descifrados son visibles para el usuario que los descarga, siempre que el usuario tenga acceso a la AWS KMS CMK.

Requisitos previos

Para exportar el contenido de buzones de correo se debe satisfacer los siguientes requisitos previos:

- Capacidad para programar.
- Una cuenta de WorkMail administrador de Amazon.
- Un bucket de Amazon S3 que no permita el acceso público. Para obtener más información, consulte Uso del bloqueo de acceso público de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service y en la Guía del usuario de Amazon Simple Storage Service.
- Una AWS KMS CMK simétrica. Para obtener más información, consulte Introducción en la Guía para desarrolladores de AWS Key Management Service .
- Un rol AWS Identity and Access Management (IAM) con una política que otorga permiso para escribir en el bucket de Amazon S3 y cifrar los archivos enviados con la AWS KMS CMK. Para obtener más información, consulte Cómo WorkMail funciona Amazon con IAM.

Ejemplos de políticas de IAM y creación de roles

El siguiente ejemplo muestra una política de IAM que concede permiso para escribir en el bucket de Amazon S3 y cifrar los archivos enviados con la AWS KMS CMK. Para utilizar esta política de ejemplo en el siguiente procedimiento de Ejemplo: Exportación del contenido de un buzón de correo, guarde la política como un archivo JSON con el nombre de archivo `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*"
                }
            }
        }
```

```
    ]
}
```

En el siguiente ejemplo se muestra una política de confianza de IAM que se vincula al rol de IAM creado. Para utilizar esta política de ejemplo en el siguiente procedimiento de Ejemplo: Exportación del contenido de un buzón de correo, guarde la política como un archivo JSON con el nombre de archivo `mailbox-export-trust-policy.json`.

No necesita utilizar las condiciones `aws:SourceArn` y `aws:SourceAccount` al mismo tiempo. Por ejemplo, puedes eliminarlo `aws:SourceArn` de la política si necesitas usar el mismo rol para exportar mensajes de diferentes WorkMail organizaciones de Amazon con la misma AWS cuenta. Para obtener más información sobre las claves de condición, consulte las Claves de contexto de condición global de AWS en la Guía del usuario de administración de identidades y accesos de AWS .

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

Puedes usar el AWS CLI para crear el rol de IAM en tu cuenta ejecutando los siguientes comandos.

```
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
```

Para obtener más información sobre el AWS CLI, consulte la Guía del AWS Command Line Interface usuario.

Ejemplo: Exportación del contenido de un buzón de correo

Después de crear el rol de IAM y las políticas en la sección anterior, complete los siguientes pasos para exportar el contenido de su buzón de correo. Debes tener tu ID de WorkMail organización de Amazon y tu ID de usuario (ID de entidad), a los que puedes acceder en la WorkMail consola de Amazon o mediante la WorkMail API de Amazon.

Ejemplo: Para exportar el contenido del buzón de correo

1. Usa el AWS CLI para iniciar el trabajo de exportación del buzón.

   ```
   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. Usa el AWS CLI para supervisar el estado de los trabajos de exportación de buzones de correo de tu WorkMail organización de Amazon.

   ```
   aws workmail list-mailbox-export-jobs --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56
   ```

   O bien, puede utilizar el ID del trabajo generado por el comando **`start-mailbox-export-job`** para monitorear solo el estado de ese trabajo de exportación de buzón de correo.

   ```
   aws workmail describe-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
   ```

Cuando el estado del trabajo de exportación del buzón es COMPLETED, los elementos del buzón de correo exportados están disponibles en un archivo `.zip` en el bucket de Amazon S3 especificado.

A continuación se muestra un ejemplo del registro de salida del buzón de correo exportado:

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportableLos artículos no son compatibles, como notas y contactos.

Consideraciones

Las siguientes consideraciones se aplican a la hora de exportar trabajos de buzones de correo para Amazon WorkMail:

- Puedes ejecutar hasta 10 trabajos de exportación de buzones de correo simultáneos para una WorkMail organización de Amazon determinada.
- Puede ejecutar un trabajo de exportación de buzón de correo para un buzón de correo determinado con una frecuencia de una vez cada 24 horas.
- Los siguientes recursos deben estar todos en la misma AWS región:
  - WorkMail Organización Amazon
  - AWS KMS CMK
  - Bucket de Amazon S3

Solución de problemas

En los temas de esta sección se explica cómo solucionar problemas en Amazon WorkMail.

Temas

Visualización de encabezados de correo electrónico

La información de los encabezados de correo electrónico puede ayudarle a solucionar problemas comunes de correo electrónico de los usuarios. Amazon te WorkMail permite ver la información del encabezado de cualquier mensaje.

Para ver los encabezados de los correos electrónicos en Amazon WorkMail

1. En la aplicación WorkMail web de Amazon, haz doble clic en el mensaje de correo electrónico para abrirlo.
2. Elija Opciones del mensaje (el icono de engranaje y sobre) situado en la esquina superior derecha del mensaje, junto a la fecha Enviado el.

Los encabezados de correo electrónico aparecen en Internet Headers (Encabezados de Internet).

Enrutamiento del correo

Si un usuario deja de recibir correos electrónicos, es posible que tu WorkMail organización de Amazon esté teniendo un problema con el enrutamiento del correo. Los pasos indicados en esta sección explican formas comunes de resolver problemas de entrega y enrutamiento.

Problemas con el correo entrante:

- Comprueba el registro MX del dominio asociado a tu WorkMail organización de Amazon. `WorkMail`debe ser la única entrada y debe tener la prioridad más baja. La existencia de múltiples registros MX podría hacer que un servicio equivocado reciba los mensajes. Para obtener más información sobre los registros MX, consulte Verificación de dominios.

- Compruebe la configuración de autenticación, informes y conformidad de mensajes basados en el dominio (DMARC) de su organización en la consola de Amazon. WorkMail Los registros DMARC se utilizan para proteger contra ataques comunes, como la suplantación de identidad o phishing, que pueden comprometer las credenciales de la cuenta de un usuario. Para obtener más información sobre DMARC, consulte Aplicación de políticas de DMARC en el correo electrónico entrante.
- Compruebe la regla de entrada de Amazon Simple Email Service. Si la regla contiene acciones distintas de Amazon WorkMail, esas acciones pueden fallar y provocar WorkMail que Amazon deje de recibir correo. Para obtener más información sobre las normas de Amazon SES, consulte Integrate with Amazon WorkMail action en la Guía para desarrolladores de Amazon Simple Email Service.
- Activa el seguimiento de mensajes en Amazon y WorkMail, a continuación, comprueba los registros para ver si hay problemas de entrega. Para obtener más información sobre el seguimiento de mensajes, consulte Habilitar el registro de eventos por correo electrónico.

Problemas con el correo saliente.

- Asegúrese de que su registro SPF incluya Amazon SES. Consulta la página de dominios en la WorkMail consola de Amazon para verificarlo. Para obtener más información sobre SPF, consulte Autenticación de correo electrónico con SPF.
- Asegúrate de que Amazon WorkMail tenga permisos para usar el dominio. De no ser así, vuelva a añadir el dominio. En esta guía, Adición de un dominio ofrece los pasos a seguir.

Cómo usar el registro diario del correo electrónico con Amazon WorkMail

Puede configurar el registro en diario para que registre sus comunicaciones a través de correo electrónico mediante archivado de terceros integrado y herramientas eDiscovery. Esto garantiza el cumplimiento de las regulaciones de cumplimiento de almacenamiento de correo electrónico para la protección de datos, el almacenamiento de datos y la protección de información.

Uso del registro histórico

Amazon WorkMail registra todos los mensajes de correo electrónico que se envían a cualquier usuario de la organización especificada, así como todos los mensajes de correo electrónico enviados por los usuarios de esa organización. Se envía una copia de todos los mensajes de correo electrónico a una dirección especificada por el administrador del sistema, en un formato denominado `journal record`. Este formato es compatible con programas de correo electrónico de Microsoft. El registro del correo en diario es gratuito.

Para el registro histórico se utilizan dos direcciones de correo electrónico: una dirección de correo electrónico de registro histórico y una dirección de correo electrónico de informe. La dirección de correo electrónico para el registro en diario es la dirección de un buzón de correo dedicado o dispositivo de terceros integrado en su cuenta, donde se envían los informes del registro en diario. La dirección de correo electrónico del informe es la dirección del administrador del sistema, donde se envían las notificaciones de los informes del registro en diario que han fallado.

Todos los registros históricos se envían desde una dirección de correo electrónico que se añade automáticamente a su dominio y que tiene el siguiente aspecto.

```
amazonjournaling@yourorganization.awsapps.com
```

No hay ningún buzón de correo asociado a esta dirección y no podrá crear uno utilizando este nombre o dirección.

> **Note**
>
> no elimine el siguiente registro de dominio de la consola de Amazon Simple Email Service (Amazon SES), o el registro histórico de correo electrónico dejará de funcionar.

```
yourorganization.awsapps.com
```

Cada mensaje de correo electrónico entrante o saliente genera un registro histórico, independientemente del número de destinatarios o grupos de usuarios. El correo electrónico que no genera un registro del diario genera una notificación de error que se envía a la dirección de correo electrónico del informe.

Para habilitar el registro en diario del correo electrónico

1. Abre la WorkMail consola de Amazon en https://console.aws.amazon.com/workmail/.

   Si es necesario, cambia la AWS región. En la barra situada en la parte superior de la ventana de la consola, abra la lista Seleccione una región y elija una región. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
2. En el panel de navegación, elija Organizaciones y, a continuación, elija el nombre de su organización.
3. En el panel de navegación, elija Configuración de la organización, la pestaña Registro histórico y luego Editar.
4. Mueva el control deslizante Estado del registro histórico a la posición activado.
5. En Dirección de correo electrónico de registro histórico, introduzca la dirección de correo electrónico proporcionada por su proveedor de registro histórico de correo electrónico.

   > **Note**
   >
   > Le recomendamos que utilice un proveedor de registro histórico dedicado.

6. En Dirección de correo electrónico de informe, introduzca la dirección del administrador de correo electrónico.
7. Seleccione Guardar. Los cambios se aplican de inmediato.

Historial de documentos

En la siguiente tabla se describen los cambios importantes en cada versión de la Guía del WorkMail administrador de Amazon. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Soporte de registro de auditorías	Los registros de auditoría se pueden utilizar para supervisar el acceso de los usuarios a los buzones de correo, auditar en busca de actividades sospechosas y depurar las configuraciones de los proveedores de control de acceso y disponibilidad. Para obtener más información, consulte Habilitar el registro de auditoría y Registrar y monitorear en Amazon WorkMail en la Guía del WorkMail administrador de Amazon.	20 de marzo de 2024
Compatibilidad con Transport Layer Security (TLS)	Amazon WorkMail dejó de ofrecer soporte para las versiones 1.0 y 1.1 de Transport Layer Security (TLS). Si utiliza TLS 1.0 o 1.1, debe actualizar la versión de TLS a la 1.2.	2 de noviembre de 2023
Usuarios remotos	Los usuarios remotos son WorkMail usuarios de Amazon alojados fuera de la WorkMail organización de Amazon o	18 de septiembre de 2023

	alojados en un dominio de correo electrónico diferente. Para obtener más información, consulte Usuarios en la Guía del WorkMail administrador de Amazon.	
Acceso programático a los buzones de correo	Amazon WorkMail ahora ofrece funciones de suplantación de identidad para conceder acceso programático a los buzones de correo. Para obtener más información, consulte Acceso programático a los buzones de correo en la Guía WorkMail del administrador de Amazon.	4 de octubre de 2022
Configurar proveedores de disponibilidad personalizados en Amazon WorkMail	Amazon WorkMail admite el uso de proveedores de disponibilidad personalizados ()CAPs. Para obtener más información, consulte Configuración de un proveedor de disponibilidad personalizado en la Guía del WorkMail administrador de Amazon.	30 de junio de 2022
Cambios en la consola para crear una organización	Se ha actualizado la experiencia de la WorkMail consola de Amazon para crear una organización. Para obtener más información, consulta Cómo crear una organización en la Guía del WorkMail administrador de Amazon.	23 de octubre de 2020

Exportación de contenido de buzones de correo	Utilice la acción de la `StartMailboxExportJob` API para exportar el contenido del WorkMail buzón de Amazon a un bucket de Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte Exportación del contenido de un buzón en la Guía WorkMail del administrador de Amazon.	22 de septiembre de 2020
Políticas de retención de buzones de correo	Establece políticas de retención de buzones para tu WorkMail organización de Amazon que eliminen automáticamente los mensajes de correo electrónico después del período de tiempo que tú elijas. Para obtener más información, consulte Configuración de políticas de retención de buzones en la Guía WorkMail del administrador de Amazon.	28 de mayo de 2020

Acciones Ejecutar Lambda sincrónicas y asincrónicas	Elija configuraciones sincrónicas o asíncronas para las acciones de Run Lambda en las reglas de flujo de correo electrónico de Amazon. WorkMail Para obtener más información, consulte Configuración AWS Lambda para Amazon WorkMail en la Guía del WorkMail administrador de Amazon.	11 de mayo de 2020
Uso de reglas de control de acceso	Las reglas de control de acceso permiten a WorkMail los administradores de Amazon controlar cómo se accede a los buzones de correo de su organización. Para obtener más información, consulta Cómo trabajar con reglas de control de acceso en la Guía del WorkMail administrador de Amazon.	12 de febrero de 2020
Etiquetado de una organización	Etiquete una WorkMail organización de Amazon para diferenciar entre las organizaciones en la Administración de facturación y costos de AWS consola o para controlar el acceso a los recursos de la organización. Para obtener más información, consulta Cómo etiquetar una organización en la Guía del WorkMail administrador de Amazon.	23 de enero de 2020

Aplicación de políticas DMARC en el correo electrónico entrante	Para obtener más información, consulte Aplicación de las políticas de DMARC en el correo electrónico entrante en la Guía del WorkMail administrador de Amazon.	17 de octubre de 2019
Recuperación de contenido de mensajes con Lambda	Utilice la API Amazon WorkMail Message Flow AWS Lambda para recuperar el contenido de los mensajes. Para obtener más información, consulte Recuperación del contenido de los mensajes con Lambda en la Guía del administrador de WorkMail Amazon.	12 de septiembre de 2019
Registro de eventos de WorkMail correo electrónico de Amazon	Activa el registro de eventos de correo electrónico en la WorkMail consola de Amazon para realizar un seguimiento de los mensajes de correo electrónico de tu organización. Para obtener más información, consulta Seguimiento de mensajes en la Guía del WorkMail administrador de Amazon.	13 de mayo de 2019

Inserción de registros DNS de Route 53	Al configurar un dominio que se administra en una zona alojada pública de Route 53, Amazon inserta WorkMail automáticamente los registros DNS por usted. Para obtener más información, consulta Cómo añadir un dominio en la Guía del WorkMail administr ador de Amazon.	13 de febrero de 2019
Configuración de Lambda para acciones de reglas de correo electrónico entrante	Amazon WorkMail admite la configuración de funciones de Lambda para usarlas con las reglas de flujo de correo entrante. Para obtener más información, consulta Cómo gestionar los flujos de correo electrónico en la Guía WorkMail del administrador de Amazon.	24 de enero de 2019
Configuración de Lambda para Amazon WorkMail	Amazon WorkMail admite la configuración de funciones de Lambda para usarlas con las reglas de flujo de correo saliente. Para obtener más información, consulte Configuración de Lambda para Amazon WorkMail en la Guía WorkMail del administrador de Amazon.	19 de noviembre de 2018

Direccionamiento SMTP	Amazon WorkMail admite la configuración de puertas de enlace SMTP para usarlas con las reglas de flujo de correo saliente. Para obtener más información, consulte Configuración de puertas de enlace SMTP en la Guía WorkMail del administrador de Amazon.	1 de noviembre de 2018
Herramientas de depuración para dominios personalizados	Amazon WorkMail ha añadido herramientas de depuración para dominios personalizados. Para obtener más informaci ón, consulta Cómo añadir un dominio en la Guía del WorkMail administrador de Amazon.	15 de octubre de 2018
Compatibilidad con Outlook 2019	Amazon WorkMail es compatible con Outlook 2019 para Windows y macOS. Para obtener más informaci ón, consulta los requisito s WorkMail del sistema de Amazon en la Guía del WorkMail administrador de Amazon.	1 de octubre de 2018
Varias actualizaciones	Varias actualizaciones en el diseño y la organización de los temas.	12 de julio de 2018

Permisos del buzón de correo	Puedes usar los permisos de buzón en Amazon WorkMail para conceder a los usuarios o grupos el derecho a trabajar en los buzones de otros usuarios. Para obtener más información, consulte Trabajar con permisos de buzones de correo en la Guía WorkMail del administrador de Amazon.	9 de abril de 2018
Support para AWS CloudTrail	Amazon WorkMail está integrado con AWS CloudTrail. Para obtener más información, consulta Cómo registrar las llamadas a la WorkMail API de Amazon AWS CloudTrail en la Guía del WorkMail administr ador de Amazon.	12 de diciembre de 2017
Soporte para flujos de correo electrónico	Puede configurar reglas de flujo de correo electróni co para administrar correo electrónico entrante en función del dominio o la dirección de correo electrónico del remitente. Para obtener más información, consulta Cómo gestionar los flujos de correo electrónico en la Guía WorkMail del administrador de Amazon.	5 de julio de 2017

Actualizaciones de la configuración rápida	Quick Setup ahora crea un WorkMail directorio de Amazon para usted. Para obtener más información, consulta Cómo configurar Amazon WorkMail con Quick Setup en la Guía del WorkMail administrador de Amazon.	10 de mayo de 2017
Soporte para una gama más amplia de clientes de correo electrónico	Ahora puedes usar Amazon WorkMail con Microsoft Outlook 2016 para Mac y clientes de correo IMAP. Para obtener más informaci ón, consulta los requisitos del sistema para Amazon WorkMail en la Guía del WorkMail administrador de Amazon.	9 de enero de 2017
Soporte para registros históricos de SMTP	Puede configurar el registro en diario para registrar su comunicación por correo electrónico. Para obtener más información, consulta Cómo usar el registro diario del correo electrónico con Amazon WorkMail en la Guía del WorkMail administrador de Amazon.	25 de noviembre de 2016

Soporte para el redirecci onamiento de correo electróni co a direcciones de correo electrónico externas	Puede configurar reglas de redireccionamiento de correo electrónico actualizando la política de identidad de Amazon SES para su dominio. Para obtener más información, consulta Editar las políticas de identidad de dominio en la Guía del WorkMail administr ador de Amazon.	26 de octubre de 2016
Soporte para interoperabilidad	Puede habilitar la interoper abilidad entre Amazon WorkMail y Microsoft Exchange. Para obtener más información, consulte Interoperabilidad entre Amazon WorkMail y Microsoft Exchange en la Guía del WorkMail administrador de Amazon.	25 de octubre de 2016
Disponibilidad general	La versión de disponibilidad general de Amazon WorkMail.	4 de enero de 2016
Soporte para reserva de recursos	Soporte para la reserva de recursos, como salas de reuniones y equipos. Para obtener más información, consulta Cómo trabajar con recursos en la Guía del WorkMail administrador de Amazon.	19 de octubre de 2015

Soporte para la herramienta de migración de correo electrónico	Soporte para la herramienta de migración de correo electrónico. Para obtener más información, consulte Migración a Amazon WorkMail en la Guía del WorkMail administrador de Amazon.	16 de agosto de 2015
Versión preliminar de Amazon WorkMail	La versión preliminar de Amazon WorkMail.	28 de enero de 2015

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.