Guia do administrador

Amazon WorkMail

Versão 1.0

Amazon WorkMail: Guia do administrador

Table of Contents

O que é a Amazon WorkMail?

WorkMail A Amazon é um serviço de e-mail e calendário empresarial seguro e gerenciado, com suporte para clientes de e-mail móveis e desktops existentes. WorkMail Os usuários da Amazon podem acessar seus e-mails, contatos e calendários usando o Microsoft Outlook, seu navegador ou seus aplicativos de e-mail nativos para iOS e Android. Você pode integrar a Amazon WorkMail ao seu diretório corporativo existente e controlar as chaves que criptografam seus dados e o local em que seus dados são armazenados.

Para ver uma lista das regiões e endpoints da AWS com suporte, consulte Regiões e endpoints da AWS.

Tópicos

Requisitos WorkMail de sistema da Amazon

Quando seu WorkMail administrador da Amazon convida você a entrar na sua WorkMail conta da Amazon, você pode entrar usando o cliente WorkMail web da Amazon.

A Amazon WorkMail também trabalha com todos os principais dispositivos móveis e sistemas operacionais compatíveis com o ActiveSync protocolo Exchange. Esses dispositivos incluem o iPad, iPhone, Android e Windows Phone. Os usuários do macOS podem adicionar sua WorkMail conta da Amazon aos aplicativos Mail, Agenda e Contatos.

A Amazon WorkMail oferece suporte às seguintes versões do sistema operacional:

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

- Windows phone — Windows 8.1 ou posterior
- Blackberry — Blackberry OS 10.3.3.3216

Se você tiver uma licença válida do Microsoft Outlook, poderá acessar a Amazon WorkMail usando as seguintes versões do Microsoft Outlook:

- Outlook 2013 ou posterior
- Outlook 2013 Clique para executar ou posterior
- Outlook para Mac 2016 ou posterior

Você pode acessar o Amazon WorkMail Web Client usando as seguintes versões de navegador:

- Google Chrome — Versão 22 ou posterior
- Mozilla Firefox — Versão 27 ou posterior
- Safari — Versão 7 ou posterior
- Internet Explorer — Versão 11
- Microsoft Edge

Você também pode usar a Amazon WorkMail com seu cliente IMAP preferido.

WorkMail Conceitos da Amazon

A terminologia e os conceitos que são fundamentais para sua compreensão e uso da Amazon WorkMail estão descritos abaixo.

Organização

Uma configuração de inquilino para a Amazon WorkMail.

Alias

Nome mundialmente exclusivo de identificação da sua organização. O alias é usado para acessar o aplicativo WorkMail web da Amazon (https://*alias* .awsapps.com/mail).

Domínio

O endereço da Web que vem após o símbolo @ em um endereço de e-mail. É possível adicionar um domínio para receber e-mails e entregá-los em caixas postais da sua organização.

Domínio de e-mail de teste

Um domínio é configurado automaticamente durante a configuração e pode ser usado para testar a Amazon WorkMail. O domínio do e-mail de teste é *alias*.awsapps.com e será usado como o domínio padrão se você não configurar seu próprio domínio. O domínio de e-mail de teste está sujeito a limites diferentes. Para ter mais informações, consulte WorkMail Cotas da Amazon.

Diretório

Um AWS Simple AD, AWS Managed AD ou AD Connector criado no AWS Directory Service. Se você criar uma organização usando a configuração do Amazon WorkMail Quick, criaremos um WorkMail diretório para você. Você não pode ver um WorkMail diretório emAWS Directory Service.

Usuário

Um usuário criado no AWS Directory Service. O usuário pode ser criado em uma função USER ou REMOTE_USER. Quando um usuário é criado e habilitado com uma função de USER, ele recebe sua própria caixa de correio para acessar. Quando um usuário está desativado, ele não pode acessar a Amazon WorkMail.

O usuário criado e habilitado com a função REMOTE_USER está listado no catálogo de endereços, mas não recebe uma caixa de correio na Amazon. WorkMail O REMOTE_USER pode ter a caixa de correio hospedada fora da Amazon WorkMail , mas ainda estará listado como qualquer outro usuário com caixa de correio no catálogo de endereços da WorkMail Amazon e poderá consultar o calendário um do outro para encontrar informações livres ou ocupadas.

Grupo

Um grupo usado no AWS Directory Service. Um grupo pode ser usado como uma lista de distribuição ou um grupo de segurança na Amazon WorkMail. Os grupos não têm suas próprias caixas de correio.

Recurso

Um recurso representa uma sala de reuniões ou um recurso de equipamento que pode ser reservado pelos WorkMail usuários da Amazon.

Política de dispositivos móveis

Várias regras de política de TI que controlam os recursos de segurança e o comportamento de um dispositivo móvel.

Serviços relacionados da AWS

Os seguintes serviços são usados junto com a Amazon WorkMail:

- AWS Directory Service—Você pode integrar a Amazon WorkMail com um AWS Simple AD, AWS Managed AD ou AD Connector existente. Crie um diretório no AWS Directory Service e, em seguida, habilite a Amazon WorkMail para esse diretório. Depois de configurar essa integração, você pode escolher quais usuários você gostaria de habilitar para a Amazon a WorkMail partir de uma lista de usuários em seu diretório atual, e os usuários podem fazer login usando suas credenciais existentes do Active Directory. Para obter mais informações, consulte Guia do administrador do AWS Directory Service.
- Amazon Simple Email Service — A Amazon WorkMail usa o Amazon SES para enviar todos os e-mails enviados. O domínio do e-mail de teste e seus domínios estão disponíveis para gerenciamento no console do Amazon SES. Não há custo para e-mails enviados pela Amazon WorkMail. Para obter mais informações, consulte Guia do desenvolvedor do Amazon Simple Storage Service.
- AWS Identity and Access Management: o AWS Management Console exige seu nome de usuário e senha para que os serviços usados possam determinar se você tem permissão para acessar os recursos. Recomendamos evitar usar as credenciais da conta da AWS para acessar a AWS, pois elas não podem ser revogadas ou limitadas. Recomendamos criar um usuário do IAM e adicioná-lo a um grupo do IAM com permissões administrativas. Assim, você pode acessar o console usando as credenciais de usuário do IAM.

  Se você tiver se cadastrado na AWS, mas não criou um usuário do IAM para você mesmo, poderá criar um usando o console do IAM. Para obter mais informações, consulte Criar um usuário do IAM individual no Guia do usuário do IAM.
- AWS Key Management Service—A Amazon WorkMail é integrada AWS KMS para criptografia dos dados do cliente. O gerenciamento principal pode ser feito no console do AWS KMS. Para obter mais informações, consulte O que é o AWS Key Management Service no Guia do desenvolvedor do AWS Key Management Service.

WorkMail Preços da Amazon

Com a Amazon WorkMail, não há taxas ou compromissos iniciais. Você paga somente pelas contas de usuário ativas. Para obter informações mais específicas sobre a definição de preço, consulte Definição de preço.

WorkMail Recursos da Amazon

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

- Aulas e workshops — Links para cursos de especialidades e baseados em perfil, bem como laboratórios autoguiados para ajudar a aperfeiçoar suas habilidades na AWS e a obter experiência prática.
- Centro dos desenvolvedores da AWS — Explore tutoriais, baixe ferramentas e informe-se sobre eventos para desenvolvedores da AWS.
- Ferramentas do desenvolvedor da AWS — Links para ferramentas de desenvolvedor, SDKs, toolkits de IDE e ferramentas da linha de comando para desenvolver e gerenciar aplicativos da AWS.
- Centro de recursos de conceitos básicos — Saiba como configurar a Conta da AWS, participar da comunidade da AWS e lançar seu primeiro aplicativo.
- Tutoriais práticos — Siga os tutoriais para iniciar seu step-by-step primeiro aplicativo no. AWS
- Whitepapers da AWS — Links para uma lista abrangente de whitepapers técnicos da AWS que abrangem tópicos como arquitetura, segurança e economia, elaborados pelos arquitetos de soluções da AWS ou por outros especialistas técnicos.
- AWS Support Center – a central para criar e gerenciar seus casos do AWS Support. Também inclui links para outros recursos úteis, como fóruns, perguntas frequentes técnicas, status de integridade do serviço e AWS Trusted Advisor.
- AWS Support— A principal página da web com informações sobre AWS Support um one-on-one canal de suporte de resposta rápida para ajudá-lo a criar e executar aplicativos na nuvem.
- Entrar em contato: um ponto central de contato para consultas relativas a faturas da AWS, contas, eventos, uso abusivo e outros problemas.
- Termos do site da AWS – informações detalhadas sobre nossos direitos autorais e marca registrada; sua conta, licença e acesso ao site, entre outros tópicos.

Pré-requisitos

Para atuar como WorkMail administrador da Amazon, você precisa de uma conta da AWS. Se você ainda não criou uma, realize as tarefas a seguir para a configuração.

Tópicos

Cadastrar-se em uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de aplicação envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

A AWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário administrativo

Depois de se inscrever em uma Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilite o AWS IAM Identity Center e crie um usuário administrativo para não usar o usuário raiz em tarefas cotidianas.

Proteger seu Usuário raiz da conta da AWS

1. Faça login no AWS Management Console como o proprietário da conta ao escolher a opção Usuário raiz e inserir o endereço de e-mail da Conta da AWS. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS.

2. Ative a autenticação multifator (MFA) para o usuário raiz.c

   Para obter instruções, consulte Habilitar um dispositivo MFA virtual para o usuário raiz de sua conta da Conta da AWS para seu (console) no Guia do usuário do IAM.

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Enabling AWS IAM Identity Center no Manual do Usuário do AWS IAM Identity Center.

2. No Centro de Identidade do IAM, conceda acesso administrativo a um usuário administrativo.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configure user access with the default Diretório do Centro de Identidade do IAM no Manual do Usuário do AWS IAM Identity Center.

Login como usuário administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda com o login utilizando um usuário do Centro de Identidade do IAM, consulte Fazer login no portal de acesso da AWS, no Guia do usuário do Início de Sessão da AWS.

Conceda permissões aos usuários do IAM para a Amazon WorkMail

Por padrão, os usuários do IAM não têm permissões para gerenciar WorkMail os recursos da Amazon. Você deve anexar uma política gerenciada pela AWS (AmazonWorkMailFullAccessou AmazonWorkMailReadOnlyAccess) ou criar uma política gerenciada pelo cliente que conceda explicitamente essas permissões aos usuários do IAM. Em seguida, anexe a política aos usuários ou grupos do IAM que precisam dessas permissões. Para ter mais informações, consulte Gerenciamento de identidade e acesso para a Amazon WorkMail.

Segurança na Amazon WorkMail

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade que se aplicam à Amazon WorkMail, consulte AWS Services in Scope by Compliance Program.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar a Amazon WorkMail. Os tópicos a seguir mostram como configurar a Amazon WorkMail para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros serviços da AWS que ajudam você a monitorar e proteger seus WorkMail recursos da Amazon.

Tópicos

Proteção de dados na Amazon WorkMail

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados na Amazon WorkMail. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com a Amazon WorkMail ou outros Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de

diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Como a Amazon WorkMail usa AWS KMS

A Amazon criptografa de WorkMail forma transparente todas as mensagens nas caixas de correio de todas as WorkMail organizações da Amazon antes que as mensagens sejam gravadas em disco, e decifra de forma transparente as mensagens quando os usuários as acessam. Você não pode desabilitar a criptografia. Para proteger as chaves de criptografia que protegem as mensagens, a Amazon WorkMail está integrada com AWS Key Management Service (AWS KMS).

A Amazon WorkMail também oferece uma opção para permitir que os usuários enviem e-mails assinados ou criptografados. Este recurso de criptografia não usa o AWS KMS. Para ter mais informações, consulte Habilitar e-mails assinados ou criptografados.

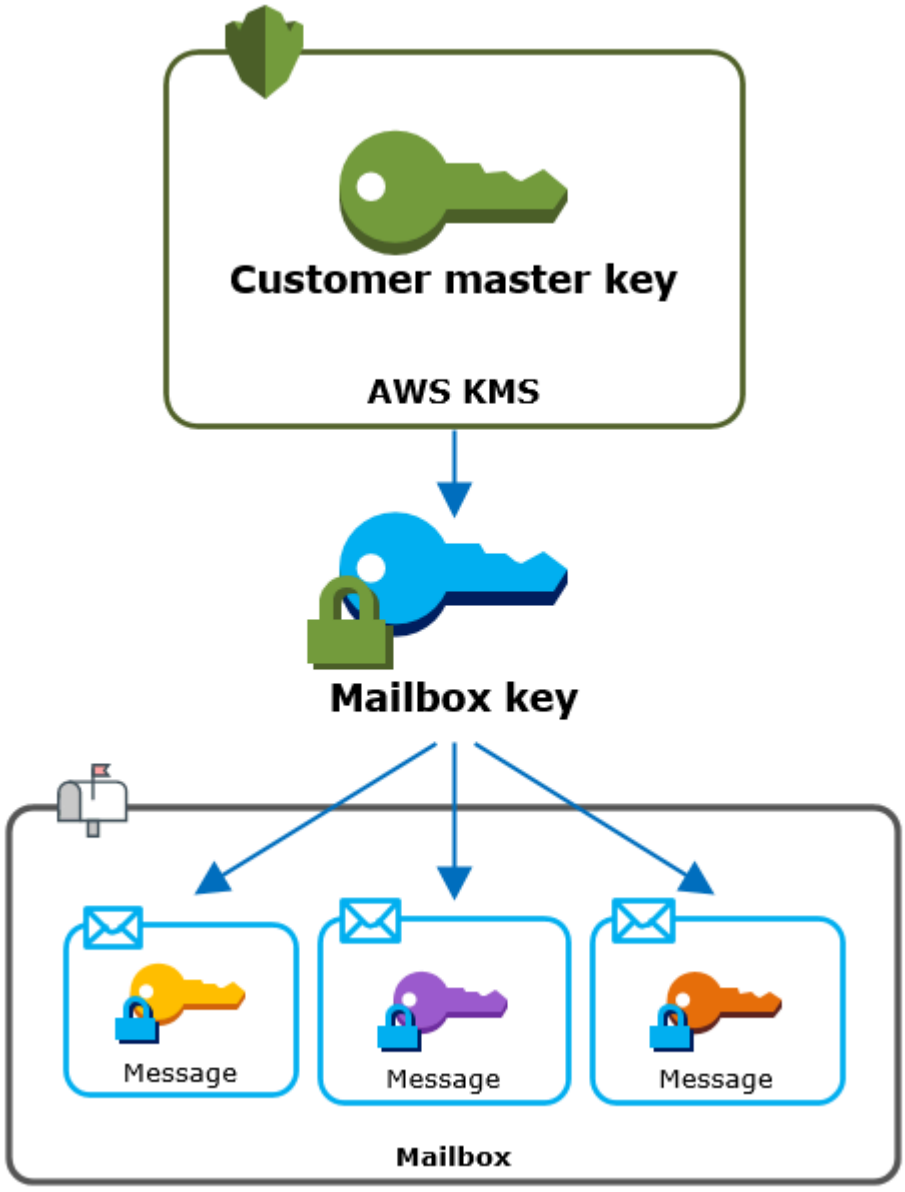
Tópicos

WorkMail Criptografia da Amazon

Na Amazon WorkMail, cada organização pode conter várias caixas de correio, uma para cada usuário na organização. Todas as mensagens, incluindo e-mail, calendário e itens são armazenados na caixa de correio do usuário.

Para proteger o conteúdo das caixas de correio em suas WorkMail organizações da Amazon, a Amazon WorkMail criptografa todas as mensagens da caixa de correio antes de serem gravadas no disco. Nenhuma informação fornecidas pelo cliente é armazenada em texto simples.

Cada mensagem é criptografada em uma chave de criptografia dos dados exclusiva. A chave da mensagem é protegida por uma chave de caixa de correio, que é uma chave exclusiva usada apenas para essa caixa de correio. A chave da caixa de correio é criptografada sob uma chave mestra AWS KMS do cliente (CMK) para a organização que nunca sai AWS KMS sem criptografia. O diagrama a seguir mostra a relação das mensagens criptografadas, chaves de mensagem criptografada, a chave de caixa de correio criptografada e a CMK para a organização no AWS KMS.



Definir uma chave KMS da organização

Ao criar uma WorkMail organização na Amazon, você tem a opção de selecionar uma chave mestra de AWS KMS cliente (CMK) para a organização. Essa CMK protege todas as chaves de correio nessa organização.

Você pode selecionar a CMK AWS gerenciada padrão para a Amazon WorkMail ou selecionar uma CMK existente gerenciada pelo cliente que você possui e gerencia. Para obter mais informações, consulte Chaves mestres do cliente (CMKs) no Guia do desenvolvedor do AWS Key Management Service . Você pode selecionar a mesma Chave KMS ou uma Chave KMS diferente para cada uma das organizações, mas não pode alterar a Chave KMS depois de selecionada.

> **Important**
>
> A Amazon WorkMail oferece suporte somente a CMKs simétricas. Não é possível usar uma Chave KMS assimétrica. Para obter ajuda para determinar se uma Chave KMS é simétrica ou assimétrica, consulte Identificar Chaves KMS simétricas e assimétricas no AWS Key Management Service Guia do desenvolvedor do .

Para encontrar a CMK da sua organização, use a entrada de AWS CloudTrail registro que registra as chamadas para AWS KMS.

Uma chave de criptografia exclusiva para cada caixa de correio

Quando você cria uma caixa de correio, a Amazon WorkMail gera uma chave de criptografia simétrica exclusiva do Advanced Encryption Standard (AES) de 256 bits para a caixa de correio, conhecida como chave de caixa de correio, fora dela. AWS KMS A Amazon WorkMail usa a chave da caixa de correio para proteger as chaves de criptografia de cada mensagem na caixa de correio.

Para proteger a chave da caixa de correio, a Amazon WorkMail liga AWS KMS para criptografar a chave da caixa de correio na CMK da organização. Ele armazena a chave de caixa de correio criptografada nos metadados da caixa de correio.

> **Note**
>
> A Amazon WorkMail usa uma chave de criptografia de caixa de correio simétrica para proteger as chaves das mensagens. Anteriormente, a Amazon WorkMail protegia cada caixa de correio com um par de chaves assimétrico. Ele usava a chave pública para criptografar cada chave de mensagem e a chave privada para descriptografá-la. A chave de caixa correio privada era protegida pela CMK para a organização. As caixas de correio mais antigas podem usar um par de chaves de caixa de correio assimétricas. Essa alteração não afeta a segurança da caixa de correio ou suas mensagens.

Criptografar de cada mensagem

Quando um usuário adiciona uma mensagem a uma caixa de correio, a Amazon WorkMail gera uma chave de criptografia simétrica AES exclusiva de 256 bits para a mensagem externa. AWS KMS Ele usa essa chave de mensagem para criptografar a mensagem. A Amazon WorkMail criptografa a chave da mensagem sob a chave da caixa de correio e armazena a chave da

mensagem criptografada com a mensagem. Ele criptografa a chave de caixa de correio na CMK para a organização.

Criar uma caixa de correio

Quando a Amazon WorkMail cria uma caixa de correio, ela usa o seguinte processo para preparar a caixa de correio para armazenar mensagens criptografadas.

- WorkMail A Amazon gera uma chave de criptografia simétrica AES exclusiva de 256 bits para a caixa de correio fora do AWS KMS.
- A Amazon WorkMail chama a operação AWS KMS Encrypt. Ele passa a chave da caixa de correio e o identificador da chave mestra do cliente (CMK) da organização. AWS KMS retorna um texto cifrado da chave da caixa de correio criptografada na CMK.
- A Amazon WorkMail armazena a chave criptografada da caixa de correio com os metadados da caixa de correio.

Criptografar uma mensagem de caixa de correio

Para criptografar uma mensagem, a Amazon WorkMail usa o seguinte processo.

1. WorkMail A Amazon gera uma chave simétrica AES exclusiva de 256 bits para a mensagem. Ele usa a chave da mensagem de texto simples e o algoritmo Advanced Encryption Standard (AES) para criptografar a mensagem fora dela. AWS KMS
2. Para proteger a chave da mensagem sob a chave da caixa de correio, a Amazon WorkMail precisa descriptografar a chave da caixa de correio, que é sempre armazenada em seu formato criptografado.

   A Amazon WorkMail chama a operação AWS KMS Decrypt e passa a chave criptografada da caixa de correio. AWS KMS usa a CMK da organização para descriptografar a chave da caixa de correio e retorna a chave da caixa de correio em texto simples para a Amazon. WorkMail
3. A Amazon WorkMail usa a chave da caixa de correio de texto simples e o algoritmo Advanced Encryption Standard (AES) para criptografar a chave da mensagem fora dela. AWS KMS
4. A Amazon WorkMail armazena a chave da mensagem criptografada nos metadados da mensagem criptografada para que esteja disponível para descriptografá-la.

Descriptografar uma mensagem de caixa de correio

Para descriptografar uma mensagem, a Amazon WorkMail usa o seguinte processo.

1. A Amazon WorkMail chama a operação AWS KMS Decrypt e passa a chave criptografada da caixa de correio. AWS KMS usa a CMK da organização para descriptografar a chave da caixa de correio e retorna a chave da caixa de correio em texto simples para a Amazon. WorkMail
2. A Amazon WorkMail usa a chave da caixa de correio de texto simples e o algoritmo Advanced Encryption Standard (AES) para descriptografar a chave da mensagem criptografada fora dela. AWS KMS
3. A Amazon WorkMail usa a chave da mensagem de texto simples para descriptografar a mensagem criptografada.

Armazenar chaves de caixa de correio em cache

Para melhorar o desempenho e minimizar as chamadas para AWS KMS, a Amazon armazena em WorkMail cache cada chave de caixa de correio de texto simples de cada cliente localmente por até um minuto. No final do período de cache, a chave de caixa de correio é removida. Se a chave da caixa de correio desse cliente for necessária durante o período de armazenamento em cache, a Amazon WorkMail poderá obtê-la do cache em vez de ligar. AWS KMS A chave de caixa de correio está protegida no cache e nunca é gravada em disco em texto simples.

Autorizar o uso da CMK

Quando a Amazon WorkMail usa uma chave mestra do cliente (CMK) em operações criptográficas, ela age em nome do administrador da caixa de correio.

Para usar a chave mestra AWS KMS do cliente (CMK) como um segredo em seu nome, o administrador deve ter as seguintes permissões. Você pode especificar essas permissões necessárias em uma política do IAM ou uma política de chaves.

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

Para permitir que a CMK seja usada somente para solicitações originadas na Amazon WorkMail, você pode usar a chave de ViaService condição kms: com o valor. `workmail.<region>.amazonaws.com`

Também é possível usar as chaves ou valores no contexto de criptografia como condição para usar a CMK em operações criptográficas. Por exemplo, você pode usar um operador de condição de string

em um documento do IAM ou de uma política de chaves, ou usar uma restrição de concessão em uma concessão.

Política de chaves para o CMK gerenciado pela AWS

A política de chaves da CMK AWS gerenciada para a Amazon WorkMail dá aos usuários permissão para usar a CMK para operações específicas somente quando a Amazon WorkMail faz a solicitação em nome do usuário. A política de chaves não permite que nenhum usuário use a CMK diretamente.

Essa política de chaves, como as políticas de todas as chaves gerenciadas pela AWS, é estabelecida pelo serviço. Não é possível alterar a política de chave, mas é possível visualizá-la a qualquer momento. Para obter mais detalhes, consulte Visualização de uma política de chave no Guia do desenvolvedor do AWS Key Management Service .

As declarações de política na política de chaves têm os seguintes efeitos:

- Permita que os usuários da conta e da região usem a CMK para operações criptográficas e criem concessões, mas somente quando a solicitação vier da Amazon WorkMail em seu nome. A chave de condição `kms:ViaService` impõe essa restrição.
- Permite que a AWS conta crie políticas do IAM que permitem aos usuários visualizar as propriedades da CMK e revogar concessões.

Veja a seguir uma política fundamental para um exemplo de CMK AWS gerenciada para a 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" : "*"
  } ]
}
```

Usando subsídios para autorizar a Amazon WorkMail

Além das principais políticas, a Amazon WorkMail usa concessões para adicionar permissões à CMK para cada organização. Para visualizar as concessões na CMK em sua conta, use a ListGrantsoperação.

A Amazon WorkMail usa concessões para adicionar as seguintes permissões à CMK da organização.

- Adicione a `kms:Encrypt` permissão para permitir que a Amazon criptografe WorkMail a chave da caixa de correio.
- Adicione a `kms:Decrypt` permissão para permitir que a Amazon use WorkMail a CMK para descriptografar a chave da caixa de correio. A Amazon WorkMail exige essa permissão em uma concessão porque a solicitação para ler mensagens da caixa de correio usa o contexto de segurança do usuário que está lendo a mensagem. A solicitação não usa as credenciais da AWS conta. WorkMail A Amazon cria essa concessão quando você seleciona uma CMK para a organização.

Para criar as doações, a Amazon WorkMail liga CreateGrantem nome do usuário que criou a organização. A permissão para criar a concessão vem de política de chaves. Essa política permite que os usuários da conta `CreateGrant` chamem a CMK da organização quando a Amazon WorkMail faz a solicitação em nome de um usuário autorizado.

A política de chaves também permite que a raiz da conta revogue a concessão da chave AWS gerenciada. No entanto, se você revogar a concessão, a Amazon não WorkMail poderá decifrar os dados criptografados em suas caixas de correio.

Contexto WorkMail de criptografia da Amazon

Um contexto de criptografia é um conjunto de pares de chave-valor que contêm dados arbitrários não secretos. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, vincula AWS KMS criptograficamente o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você deve passar o mesmo contexto de criptografia. Para obter mais informações, consulte Contexto de criptografia no Guia do desenvolvedor AWS Key Management Service .

A Amazon WorkMail usa o mesmo formato de contexto de criptografia em todas as operações AWS KMS criptográficas. É possível usar o contexto de criptografia para identificar uma operação criptográfica em logs e registros de auditoria, como o AWS CloudTrail, e como uma condição para a autorização em políticas e concessões.

Em suas solicitações de criptografia e descriptografia, a AWS KMS Amazon WorkMail usa um contexto de criptografia em que a chave está `aws:workmail:arn` e o valor é o Amazon Resource Name (ARN) da organização.

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

Por exemplo, o seguinte contexto de criptografia inclui um exemplo de ARN da organização na região Europa (Irlanda) (`eu-west-1`).

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

Monitorando a WorkMail interação da Amazon com AWS KMS

Você pode usar o AWS CloudTrail Amazon CloudWatch Logs para rastrear as solicitações que a Amazon WorkMail envia AWS KMS em seu nome.

Encrypt

Quando você cria uma caixa de correio, a Amazon WorkMail gera uma chave de caixa de correio e liga AWS KMS para criptografar a chave da caixa de correio. WorkMail A Amazon envia uma solicitação Encrypt AWS KMS com a chave da caixa de correio em texto simples e um identificador para a CMK da organização Amazon. WorkMail

O evento que registra a operação `Encrypt` é semelhante ao evento de exemplo a seguir. O usuário é o WorkMail serviço da Amazon. Os parâmetros incluem o CMK ID (`keyId`) e o contexto de

criptografia da WorkMail organização Amazon. A Amazon WorkMail também passa a chave da caixa de correio, mas isso não é registrado no CloudTrail registro.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestID": "76e96b96-7e24-4faf-a2d6-08ded2eaf63c",
    "eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```

Decrypt

Quando você adiciona, visualiza ou exclui uma mensagem da caixa de correio, a Amazon WorkMail pede AWS KMS para descriptografar a chave da caixa de correio. WorkMail A Amazon envia uma solicitação Decrypt AWS KMS com a chave criptografada da caixa de correio e um identificador para a CMK da organização Amazon. WorkMail

O evento que registra a operação `Decrypt` é semelhante ao evento de exemplo a seguir. O usuário é o WorkMail serviço da Amazon. Os parâmetros incluem a chave criptografada da caixa de correio (como um blob de texto cifrado), que não é registrada no log, e o contexto de criptografia da organização Amazon. WorkMail AWS KMS deriva o ID da CMK do 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"
}
```

Gerenciamento de identidade e acesso para a Amazon WorkMail

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos da Amazon WorkMail . O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz na Amazon WorkMail.

Usuário do serviço — Se você usa o WorkMail serviço da Amazon para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais WorkMail recursos da Amazon para fazer seu trabalho, você pode precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso na Amazon WorkMail, consulteSolução de problemas de WorkMail identidade e acesso da Amazon.

Administrador de serviços — Se você é responsável pelos WorkMail recursos da Amazon em sua empresa, provavelmente tem acesso total à Amazon WorkMail. É seu trabalho determinar quais WorkMail recursos e recursos da Amazon seus usuários do serviço devem acessar. Assim, você

deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com a Amazon WorkMail, consulteComo a Amazon WorkMail trabalha com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso à Amazon WorkMail. Para ver exemplos de políticas WorkMail baseadas em identidade da Amazon que você pode usar no IAM, consulte. Exemplos de políticas WorkMail baseadas em identidade da Amazon

Autenticar com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário. Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis.. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando

uma URL personalizada. Para mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas – É possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do

IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para mais informações sobre Organizações e SCPs, consulte Como os SCPs funcionam no AWS Organizations Guia do Usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas

substitui a permissão. Para mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como a Amazon WorkMail trabalha com o IAM

Antes de usar o IAM para gerenciar o acesso à Amazon WorkMail, você deve entender quais recursos do IAM estão disponíveis para uso com a Amazon WorkMail. Para ter uma visão de alto nível de como a Amazon WorkMail e outros AWS serviços funcionam com o IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Tópicos

- Políticas baseadas em WorkMail identidade da Amazon
- Políticas baseadas em WorkMail recursos da Amazon
- Autorização baseada em WorkMail tags da Amazon
- Funções WorkMail do Amazon IAM

Políticas baseadas em WorkMail identidade da Amazon

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. A Amazon WorkMail oferece suporte a ações, recursos e chaves de condição específicos. Para conhecer todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de

AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações políticas na Amazon WorkMail usam o seguinte prefixo antes da ação:`workmail:`. Por exemplo, para conceder permissão a alguém para recuperar uma lista de usuários com a operação de WorkMail `ListUsers` API da Amazon, você inclui a `workmail:ListUsers` ação na política dessa pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. A Amazon WorkMail define seu próprio conjunto de ações que descrevem tarefas que você pode realizar com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

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

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a seguinte ação:

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

Para ver uma lista de WorkMail ações da Amazon, consulte Ações definidas pela Amazon WorkMail no Guia do usuário do IAM.

Recursos

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento de política `Resource` JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

A Amazon WorkMail oferece suporte a permissões em nível de recursos para organizações da Amazon. WorkMail

O recurso WorkMail organizacional da Amazon tem o seguinte ARN:

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

Para obter mais informações sobre o formato dos ARNs, consulte Amazon Resource Names (ARNs) e namespaces AWS de serviços.

Por exemplo, para especificar a organização `m-n1pq2345678r901st2u3vx45x6789yza` em sua declaração, use o ARN a seguir.

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

Para especificar todas as organizações que pertencem a uma conta específica, use o caractere curinga (*):

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

Algumas WorkMail ações da Amazon, como aquelas para criar recursos, não podem ser realizadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

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

Para ver uma lista dos tipos de WorkMail recursos da Amazon e seus ARNs, consulte Recursos definidos pela Amazon WorkMail no Guia do usuário do IAM. Para saber com quais ações você pode especificar para o ARN de cada recurso, consulte Ações, recursos e chaves de condição para a Amazon. WorkMail

Chaves de condição

A Amazon WorkMail oferece suporte às seguintes chaves de condição globais.

- `aws:CurrentTime`

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

O exemplo de política a seguir concede acesso ao WorkMail console da Amazon somente de diretores do IAM autenticados pelo MFA na região da 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 as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

`workmail:ImpersonationRoleId`é a única chave de condição específica do serviço suportada pela Amazon. WorkMail

O exemplo a seguir reduz o escopo da `AssumeImpersonationRole` ação para uma determinada WorkMail organização e função de representação.

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

Exemplos

Para ver exemplos de políticas WorkMail baseadas em identidade da Amazon, consulte. Exemplos de políticas WorkMail baseadas em identidade da Amazon

Políticas baseadas em WorkMail recursos da Amazon

A Amazon WorkMail não oferece suporte a políticas baseadas em recursos.

Autorização baseada em WorkMail tags da Amazon

Você pode anexar tags aos WorkMail recursos da Amazon ou passar tags em uma solicitação para a Amazon WorkMail. Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Para obter mais informações sobre a marcação de WorkMail recursos da Amazon, consulteMarcar uma organização.

Funções WorkMail do Amazon IAM

Uma função do IAM é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com a Amazon WorkMail

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

A Amazon WorkMail oferece suporte ao uso de credenciais temporárias.

Perfis vinculados ao serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. Os perfis vinculados a serviço aparecem na sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

A Amazon WorkMail oferece suporte a funções vinculadas a serviços. Para obter detalhes sobre como criar ou gerenciar funções WorkMail vinculadas a serviços da Amazon, consulte. Usar funções vinculadas ao serviço no Amazon WorkMail

Perfis de serviço

Esse atributo permite que um serviço assuma um perfil de serviço em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. Os perfis de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso indica que um administrador do IAM pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

A Amazon WorkMail oferece suporte a funções de serviço.

Exemplos de políticas WorkMail baseadas em identidade da Amazon

Por padrão, os usuários e funções do IAM não têm permissão para criar ou modificar WorkMail recursos da Amazon. Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM utilizando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir WorkMail recursos da Amazon em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para mais informações, consulte Elementos da política JSON do IAM: condição no Manual do Usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o WorkMail console da Amazon

Para acessar o WorkMail console da Amazon, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os WorkMail recursos da Amazon em sua AWS conta. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis do IAM) com essa política.

Para garantir que essas entidades ainda possam usar o WorkMail console da Amazon, anexe também a seguinte política AWS gerenciada AmazonWorkMailFullAccess,, às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

A AmazonWorkMailFullAccesspolítica concede a um usuário do IAM acesso total aos WorkMail recursos da Amazon. Essa política dá ao usuário acesso a todas as AWS Directory Service operações e serviços da Amazon Simple Email Service. WorkMail AWS Key Management Service

Isso também inclui várias operações do Amazon EC2 que a Amazon WorkMail precisa realizar em seu nome. As `cloudwatch` permissões `logs` e são necessárias para e-mail, registro de eventos e visualização de métricas no WorkMail console da Amazon. O registro de auditoria usa CloudWatch Logs, Amazon S3 e Amazon Data FireHose para armazenar. `logs` Para ter mais informações, consulte Registro e monitoramento na 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"
            }
        }
    }
  ]
}
```

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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": "*"
        }
    ]
}
```

Permita que os usuários tenham acesso somente para leitura aos recursos da Amazon WorkMail

A declaração de política a seguir concede a um usuário do IAM acesso somente de leitura aos recursos da Amazon WorkMail. Essa política fornece o mesmo nível de acesso que a política gerenciada da AWS AmazonWorkMailReadOnlyAccess. Qualquer uma das políticas dá ao usuário acesso a todas as WorkMail `Describe` operações da Amazon. O acesso à AWS Directory Service `DescribeDirectories` operação é necessário para obter informações sobre seus AWS Directory Service diretórios. O acesso ao serviço do Amazon SES é necessário para obter informações sobre os domínios configurados. O acesso a AWS Key Management Service é necessário para obter informações sobre as chaves de criptografia usadas. As `cloudwatch` permissões `logs` e são necessárias para registrar eventos por e-mail e visualizar métricas no WorkMail console da Amazon. O registro de auditoria usa CloudWatch Logs, Amazon S3 e Amazon Data FireHose para armazenar. `logs` Para ter mais informações, consulte Registro e monitoramento na 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": "*"
    }
  ]
}
```

Solução de problemas de WorkMail identidade e acesso da Amazon

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com a Amazon WorkMail e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação na Amazon WorkMail
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha AWS conta acessem meus WorkMail recursos da Amazon

Não estou autorizado a realizar uma ação na Amazon WorkMail

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

O exemplo de erro a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um grupo, mas não tem as permissões de `workmail:DescribeGroup`.

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

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso `group` usando a ação `workmail:DescribeGroup`.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para a Amazon WorkMail.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação na Amazon WorkMail. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha AWS conta acessem meus WorkMail recursos da Amazon

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se a Amazon WorkMail oferece suporte a esses recursos, consulteComo a Amazon WorkMail trabalha com o IAM.

- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

AWS políticas gerenciadas para a Amazon WorkMail

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos atributos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e perfis) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo atributo for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e

descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

AWS política gerenciada: AmazonWorkMailFullAccess

É possível anexar a política `AmazonWorkMailFullAccess` a suas identidades do IAM. Essa política concede permissões que permitem acesso total à Amazon WorkMail.

Para ver as permissões dessa política, consulte AmazonWorkMailFullAccessno AWS Management Console.

AWS política gerenciada: AmazonWorkMailReadOnlyAccess

É possível anexar a política `AmazonWorkMailReadOnlyAccess` a suas identidades do IAM. Essa política concede permissões que permitem acesso somente para leitura à Amazon. WorkMail

Para ver as permissões dessa política, consulte AmazonWorkMailReadOnlyAccessno AWS Management Console.

AWS política gerenciada: AmazonWorkMailEventsServiceRolePolicy

Essa política é anexada à função vinculada ao serviço nomeada AmazonWorkMailEventspara permitir o acesso aos AWS serviços e recursos usados ou gerenciados pelos eventos da Amazon WorkMail . Para ter mais informações, consulte Usar funções vinculadas ao serviço no Amazon WorkMail.

WorkMail Atualizações da Amazon para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas da Amazon WorkMail desde que esse serviço começou a monitorar essas mudanças.

Alteração	Descrição	Data
Atualizações de políticas gerenciadas pela AWS — Atualização de uma política existente	As `AmazonWorkMailFullAccess` permissões `AmazonWorkMailReadOnlyAccess` e foram atualizadas para que WorkMail a Amazon ofereça	14 de fevereiro de 2024

Alteração	Descrição	Data
	suporte ao registro de auditoria. Para obter mais informações sobre as permissões atualizadas, consulte Exemplos de políticas WorkMail baseadas em identidade da Amazon e para obter informações sobre o registro de auditoria, consulteHabilitando o registro de auditoria.	
A Amazon WorkMail começou a monitorar as mudanças	A Amazon WorkMail começou a monitorar as mudanças em suas políticas AWS gerenciadas.	1º de março de 2021

Usar funções vinculadas ao serviço no Amazon WorkMail

O Amazon WorkMail usa funções vinculadas ao serviço do AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo especial de perfil do IAM vinculado diretamente ao Amazon WorkMail. As funções vinculadas a serviços são predefinidas pelo Amazon WorkMail e incluem todas as permissões que o serviço precisa para chamar outros produtos da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do Amazon WorkMail porque você não precisa adicionar as permissões necessárias manualmente. O Amazon WorkMail define as permissões das funções vinculadas ao serviço e, exceto definido de outra forma, somente o Amazon WorkMail pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir uma função vinculada ao serviço somente depois de excluir os recursos relacionados da . Isso protege os recursos do Amazon WorkMail, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte às funções vinculadas a serviço, consulte Serviços da AWS compatíveis que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Função vinculada ao serviço. Escolha um Sim com um link para exibir a documentação da função vinculada a serviço desse serviço.

Permissões da função vinculada ao serviço no Amazon WorkMail

O Amazon WorkMail usa a função vinculada ao serviço chamada AmazonWorkmailEvents – O Amazon WorkMail usa essa função vinculada ao serviço para permitir o acesso a serviços e recursos da AWS usados ou gerenciados por eventos do Amazon WorkMail, como o monitoramento de eventos de e-mail registrados em log pelo CloudWatch. Para obter mais informações sobre como habilitar o registro em log de eventos de e-mail no Amazon WorkMail, consulte Habilitando o registro de eventos de e-mail.

A função vinculada ao serviço AmazonWorkMailEvents confia nos seguintes serviços para assumir a função:

- `events.workmail.amazonaws.com`

A política de permissões da função permite que o Amazon WorkMail conclua as ações a seguir nos recursos especificados:

- Ação: `logs:CreateLogGroup` em `all AWS resources`
- Ação: `logs:CreateLogStream` em `all AWS resources`
- Ação: `logs:PutLogEvents` em `all AWS resources`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Service-linked role permissions (Permissões de função vinculada a serviços) no Guia do usuário do IAM.

Criar uma função vinculada ao serviço no Amazon WorkMail

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você ativa o registro em log de eventos do Amazon WorkMail e usa as configurações padrão no console do Amazon WorkMail, o Amazon WorkMail cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você ativa o registro em log de eventos do Amazon WorkMail e usa as configurações padrão, o Amazon WorkMail cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada ao serviço no Amazon WorkMail

O Amazon WorkMail não permite que você edite a função vinculada ao serviço AmazonWorkMailEvents. Depois que você criar uma função vinculada a serviço, não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, você poderá editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço no Amazon WorkMail

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o serviço do Amazon WorkMail estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do Amazon WorkMail usados por AmazonWorkMailEvents

1. Desative o registro em log de eventos do Amazon WorkMail.

   a. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

      Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.

   b. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.

c. No painel de navegação, selecione Configurações da organização e, em seguida, escolha Monitoramento.

d. Em Log settings (Configurações de log), escolha Edit (Editar).

e. Mova o controle deslizante Habilitar eventos de e-mail para a posição desativado.

f. Escolha Save (Salvar).

2. Excluir o grupo de logs do Amazon CloudWatch.

a. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.

b. Escolha Logs.

c. Em Log Groups (Grupos de log), selecione os grupos para excluir.

d. Em Actions (Ações), escolha Delete log group (Excluir grupo de registros).

e. Selecione Sim, excluir.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada ao serviço AmazonWorkMailEvents. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões compatíveis com funções vinculadas ao serviço do Amazon WorkMail

O Amazon WorkMail é compatível com funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints do Amazon WorkMail.

Registro e monitoramento na Amazon WorkMail

Monitorar e auditar seus e-mails e registros é importante para manter a saúde da sua WorkMail organização na Amazon. A Amazon WorkMail oferece suporte a dois tipos de monitoramento:

- Registro de eventos — O monitoramento da atividade de envio de e-mails da sua organização ajuda a proteger a reputação do seu domínio. O monitoramento também pode ajudar a rastrear os e-mails enviados e recebidos. Para obter mais informações sobre como habilitar o registro de eventos de e-mail, consulte Habilitando o registro de eventos de e-mail.

- Registro de auditoria — Você pode usar registros de auditoria para capturar informações detalhadas sobre o uso WorkMail da sua organização na Amazon, como monitorar o acesso do usuário às caixas de correio, auditar atividades suspeitas e depurar configurações do provedor de disponibilidade e controle de acesso. Para ter mais informações, consulte Habilitando o registro de auditoria.

AWS fornece as seguintes ferramentas de monitoramento para monitorar a Amazon WorkMail, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos nos quais você executa AWS em tempo real. Por exemplo, quando você ativa o registro de eventos de e-mail para a Amazon WorkMail, CloudWatch pode rastrear e-mails enviados e recebidos para sua organização. Para obter mais informações sobre o monitoramento da Amazon WorkMail com CloudWatch, consulteMonitorando a Amazon WorkMail com CloudWatch métricas. Para obter mais informações sobre CloudWatch, consulte o Guia CloudWatch do usuário da Amazon.
- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus eventos de e-mail e registros de auditoria para a Amazon WorkMail quando o e-mail e o registro de auditoria estão habilitados no WorkMail console da Amazon. CloudWatch Os registros podem monitorar as informações nos arquivos de log e você pode arquivar seus dados de log em um armazenamento altamente durável. Para obter mais informações sobre o rastreamento de WorkMail mensagens da Amazon usando CloudWatch Logs, consulte Habilitando o registro de eventos de e-mail Habilitando o registro de auditoria e. Para obter mais informações sobre CloudWatch registros, consulte o Guia do usuário do Amazon CloudWatch Logs.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por você ou em seu Conta da AWS nome e entrega os arquivos de log em um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para ter mais informações, consulte Registrando chamadas de WorkMail API da Amazon com AWS CloudTrail.
- O Amazon S3 permite que você armazene e acesse seus WorkMail eventos da Amazon de forma econômica. O Amazon S3 fornece mecanismos para gerenciar o ciclo de vida dos dados do evento, permitindo que você configure a exclusão automática de eventos antigos ou configure o arquivamento automático no Amazon S3 Glacier. Observe que a entrega do Amazon S3 só está disponível para eventos de registro de auditoria. Para obter mais informações sobre o Amazon S3, consulte o Guia do usuário da Amazon S3.
- O Amazon Data Firehose permite que você transmita seus dados de eventos para outros serviços da AWS, como Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Service,

Amazon Serverless OpenSearch , Splunk e qualquer endpoint HTTP personalizado ou endpoints HTTP de propriedade de provedores de serviços terceirizados compatíveis, incluindo Datadog LogicMonitor, Dynatrace, MongoDB, New Relic, Coralogix e Elastic. OpenSearch A entrega para o Firehose só está disponível para eventos de registro de auditoria. Para obter mais informações sobre o Firehose, consulte o guia do desenvolvedor do Amazon Data Firehose.

Tópicos

Monitorando a Amazon WorkMail com CloudWatch métricas

Você pode monitorar a Amazon WorkMail usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. As métricas gratuitas são armazenadas por 15 meses para que você possa acessar informações históricas para ver o desempenho de seu aplicativo ou serviço web. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

CloudWatch métricas para a Amazon WorkMail

WorkMailA Amazon envia as seguintes informações de métricas e dimensões para CloudWatch.

O namespace `AWS/WorkMail` inclui as métricas a seguir.

Métrica	Descrição
`OrganizationEmailReceived`	O número de e-mails recebidos pela sua WorkMail organização Amazon. Se um e-mail for endereçado a 10 destinatários em

Métrica	Descrição
	sua organização, a `OrganizationEmailReceived` contagem será de um. Unidades: contagem
`MailboxEmailDelivered`	O número de e-mails enviados para caixas de correio individuais em sua WorkMail organização Amazon. Se um e-mail for entregue com sucesso a 10 destinatários em sua organização, a `MailboxEmailDelivered` contagem será 10. Unidades: contagem
`IncomingEmailBounced`	Número de e-mails recebidos que foram devolvidos devido a caixas de correio cheias. Essa métrica conta para cada destinatário pretendido. Por exemplo, se um e-mail for enviado para 10 destinatários em sua organização e dois dos destinatários tiverem caixas de correio cheias, resultando em uma resposta de devolução, a `IncomingEmailBounced` contagem será duas. Unidades: contagem
`OutgoingEmailBounced`	O número de e-mails enviados que não puderam ser entregues. Essa métrica conta para cada destinatário pretendido. Por exemplo, se um e-mail for enviado para 10 destinatários e dois e-mails não puderem ser entregues, a `OutgoingEmailBounced` contagem será 2. Unidades: contagem

Métrica	Descrição
`OutgoingEmailSent`	O número de e-mails enviados com sucesso pela sua WorkMail organização Amazon. Essa métrica conta para cada destinatário de um e-mail enviado com êxito. Por exemplo, se 1 e-mail é enviado para 10 destinatários, e é entregue com êxito para 8 destinatários, a contagem de `OutgoingEmailSent` é 8. Unidades: contagem
`AuthenticationFailure`	Essa métrica conta o número de tentativas de autenticação. Quando a autenticação é bem-sucedida, a contagem é 0 e quando a autenticação não é bem-sucedida, a contagem é 1. Use a `Sum` estatística para monitorar a quantidade de tentativas de autenticação malsucedidas. Use a `Sample count` estatística para monitorar o número total de eventos de autenticação. Use a `Average` estatística para monitorar a proporção de eventos de autenticação fracassados e bem-sucedidos. Unidades: contagem
`AccessDenied`	Essa métrica conta o número de avaliações de controle de acesso. Quando a ação é negada pelo controle de acesso, a contagem é 1 e quando a ação é concedida, a contagem é 0. Use a `Sum` estatística para monitorar o volume de ações negadas, a `Sample count` estatística para monitorar o número total de ações tentadas e a `Average` estatística para monitorar a proporção de ações permitidas e negadas. Unidades: contagem

Métrica	Descrição
`ActionDenied`	Essa métrica é contada quando há ação nos dados da caixa de correio. Quando a ação é negada, a contagem é 1 e, se a ação for concedida, a contagem será 0. Use a `Sum` estatística para monitorar o volume de ações negadas na caixa de correio, a `Sample count` estatística para monitorar o número total de tentativas de ações na caixa de correio e a `Average` estatística para monitorar a proporção de ações permitidas e negadas. Unidades: contagem
`AvailabilityProviderFailure`	Essa métrica é contabilizada para cada solicitação de provedor de disponibilidade que a Amazon WorkMail executa para recuperar a disponibilidade do calendário de uma fonte externa. Para obter mais informações sobre provedores de disponibilidade, consulte o Amazon WorkMail Administrator Guide.

Monitorando registros WorkMail de eventos de e-mail da Amazon

Quando você ativa o registro de eventos de e-mail para sua WorkMail organização Amazon, a Amazon WorkMail registra eventos de e-mail com CloudWatch. Para obter mais informações sobre como habilitar o registro de eventos de e-mail em log, consulte Habilitando o registro de eventos de e-mail.

As tabelas a seguir descrevem os eventos com WorkMail os quais a Amazon registra CloudWatch, quando os eventos são transmitidos e o que os campos de eventos contêm.

`ORGANIZATION_EMAIL_RECEIVED`

Esse evento é registrado quando sua WorkMail organização Amazon recebe uma mensagem de e-mail.

Campo	Descrição
recipients	Os destinatários pretendidos na mensagem.
sender (remetente)	O endereço de e-mail do usuário que enviou a mensagem de e-mail em nome de outro usuário. Esse campo é definido somente quando um e-mail é enviado em nome de outro usuário.
from	O endereço De, que normalmente corresponde ao endereço de e-mail do usuário que enviou a mensagem. Se o usuário enviou a mensagem como outro usuário ou em nome de outro usuário, esse campo retorna o endereço de e-mail do usuário em cujo nome a mensagem foi enviada, e não o endereço do remetente real.
subject	O assunto da mensagem do e-mail.
messageId	O ID da mensagem SMTP
spamVerdict	Indica se a mensagem foi marcada como spam pelo Amazon SES. Para obter mais informaçõ es, consulte Conteúdo de notificações para o recebimento de e-mails do Amazon SES no Guia do desenvolvedor do Amazon Simple Email Service.
dkimVerdict	Indica se a verificação de correio DomainKey s identificado (DKIM) foi aprovada. Para obter mais informações, consulte Conteúdo de notificações para o recebimento de e-mails do Amazon SES no Guia do desenvolvedor do Amazon Simple Email Service.
dmarcVerdict	Indica se a verificação de Autenticação, Relatórios e Conformidade de Mensagens

Campo	Descrição
	Baseada em Domínio (DMARC) foi aprovada. Para obter mais informações, consulte Conteúdo de notificações para o recebimento de e-mails do Amazon SES no Guia do desenvolvedor do Amazon Simple Email Service.
dmarcPolicy	Aparece somente quando o campo dmarcVerdict contém "FAIL". Indica a ação a ser executada no e-mail quando ocorre falha na verificação de DMARC (NONE (Nenhuma), QUARANTINE (Quarentena) ou REJECT (Rejeitar)). Isso é definido pelo proprietário do domínio de envio de e-mail.
spfVerdict	Indica se as verificações do Sender Policy Framework (SPF) foram aprovadas. Para obter mais informações, consulte Conteúdo de notificações para o recebimento de e-mails do Amazon SES no Guia do desenvolvedor do Amazon Simple Email Service.
messageTimestamp	Indica quando a mensagem é recebida.

`MAILBOX_EMAIL_DELIVERED`

Esse evento é registrado quando uma mensagem é enviada a uma caixa de correio na sua organização. É registrado uma vez para cada caixa à qual a mensagem é entregue, portanto, um único evento `ORGANIZATION_EMAIL_RECEIVED` pode resultar em vários eventos `MAILBOX_EMAIL_DELIVERED`.

Campo	Descrição
recipient (destinatário)	A caixa de correio à qual a mensagem é entregue.

Campo	Descrição
folder	A pasta da caixa de correio onde a mensagem é colocada.

`RULE_APPLIED`

Esse evento é registrado quando uma mensagem recebida ou enviada inicia uma regra de fluxo de e-mail.

Campo	Descrição
ruleName	O nome da regra.
ruleType	O tipo de regra aplicada (INBOUND_RULE, OUTBOUND_RULE ou MAILBOX_RULE). As regras de entrada e saída se aplicam à sua organização Amazon WorkMail. As regras de caixa de correio se aplicam a caixas específicas. Para ter mais informações, consulte Gerenciar fluxos de e-mail.
ruleActions	Ações realizadas com base na regra. Diferentes destinatários da mensagem podem ter ações diferentes, como um e-mail devolvido ou um e-mail entregue com êxito.
targetFolder	Pasta de destino pretendida para um MAILBOX_RULE `Move` ou `Copy`.
targetRecipient	Destinatário pretendido de um MAILBOX_RULE `Forward` ou `Redirect`.

`JOURNALING_INITIATED`

Esse evento é registrado quando a Amazon WorkMail envia um e-mail para o endereço de registro no diário especificado pelo administrador da sua organização. Só é transmitido se o registro em log

estiver configurado para a sua organização. Para ter mais informações, consulte Usando o registro no diário de e-mail com o Amazon WorkMail.

Campo	Descrição
journalingAddress	Endereço de e-mail para o qual a mensagem de registro é enviada.

INCOMING_EMAIL_BOUNCED

Esse evento é registrado em log quando uma mensagem recebida não pode ser entregue a um destinatário. Os e-mails podem ser devolvidos por vários motivos, como uma caixa de correio de destino cheia. IO sistema registra em log esse evento uma vez para cada destinatário que resultou em um e-mail devolvido. Por exemplo, se uma mensagem recebida é direcionada a três destinatários, e dois deles estão com a caixa cheia, dois eventos INCOMING_EMAIL_BOUNCED são registrados.

Campo	Descrição
bouncedRecipient	O destinatário pretendido para o qual a Amazon WorkMail devolveu a mensagem.

OUTGOING_EMAIL_SUBMITTED

Esse evento é registrado quando um usuário na sua organização gera uma mensagem de envio de e-mail. Isso é registrado antes que a mensagem saia da Amazon WorkMail, portanto, esse evento não indica se o e-mail foi entregue com sucesso.

Campo	Descrição
recipients	Os destinatários da mensagem conforme especificado pelo remetente. Inclui todos os destinatários no campos Para, Cc e Cco.
sender (remetente)	O endereço de e-mail do usuário que enviou a mensagem de e-mail em nome de outro usuário. Esse campo é definido somente

Campo	Descrição
	quando um e-mail é enviado em nome de outro usuário.
from	O endereço De, que normalmente corresponde ao endereço de e-mail do usuário que enviou a mensagem. Se o usuário enviou a mensagem como outro usuário ou em nome de outro usuário, esse campo retorna o endereço de e-mail do usuário em cujo nome a mensagem foi enviada, e não o endereço do remetente real.
subject	O assunto da mensagem do e-mail.

`OUTGOING_EMAIL_SENT`

Esse evento é registrado quando um e-mail enviado é entregue para um destinatário esperado. É registrado uma vez para cada entrega bem-sucedida, portanto, um único `OUTGOING_EMAIL_SUBMITTED` pode resultar em várias entradas `OUTGOING_EMAIL_SENT`.

Campo	Descrição
recipient (destinatário)	O destinatário do e-mail entregue com êxito.
sender (remetente)	O endereço de e-mail do usuário que enviou a mensagem de e-mail em nome de outro usuário. Esse campo é definido somente quando um e-mail é enviado em nome de outro usuário.
from	O endereço De, que normalmente corresponde ao endereço de e-mail do usuário que enviou a mensagem. Se o usuário enviou a mensagem como outro usuário ou em nome de outro usuário, esse campo retorna o endereço de e-mail do usuário em cujo nome a mensagem foi enviada, e não o endereço do remetente real.

Campo	Descrição
messageId	O ID da mensagem SMTP

OUTGOING_EMAIL_BOUNCED

Esse evento é registrado em log quando uma mensagem enviada não pode ser entregue a um destinatário. Os e-mails podem ser devolvidos por vários motivos, como uma caixa de correio de destino cheia. O sistema registra em log uma devolução para cada destinatário que resulta em um e-mail devolvido. Por exemplo, se uma mensagem enviada é direcionada a três destinatários, e dois deles estão com as caixas cheias, dois eventos `OUTGOING_EMAIL_BOUNCED` são registrados.

Campo	Descrição
bouncedRecipient	O destinatário esperado do qual o servidor de destino enviou a mensagem de devolução.

DMARC_POLICY_APPLIED

Esse evento é registrado em log quando uma política DMARC é aplicada a um e-mail enviado à sua organização.

Campo	Descrição
from	O endereço De, que normalmente corresponde ao endereço de e-mail do usuário que enviou a mensagem. Se o usuário enviou a mensagem como outro usuário ou em nome de outro usuário, esse campo retorna o endereço de e-mail do usuário em cujo nome a mensagem foi enviada, e não o endereço do remetente real.
recipients	Os destinatários pretendidos na mensagem.
política	A política DMARC aplicada, indicando a ação a ser executada no e-mail quando ocorre falha na verificação de DMARC (NONE

Campo	Descrição
	(Nenhuma), QUARANTINE (Quarentena) ou REJECT (Rejeitar)). É o mesmo que o campo dmarcPolicy no evento ORGANIZATION_EMAIL_RECEIVED.

Monitoramento dos registros WorkMail de auditoria da Amazon

Você pode usar registros de auditoria para monitorar o acesso às caixas de correio da sua WorkMail organização Amazon. A Amazon WorkMail registra quatro tipos de eventos de auditoria e esses eventos podem ser publicados no CloudWatch Logs, no Amazon S3 ou no Amazon Firehouse. Você pode usar registros de auditoria para monitorar a interação do usuário com as caixas de correio da sua organização, as tentativas de autenticação, a avaliação das regras de controle de acesso e realizar chamadas do provedor de disponibilidade para sistemas externos. Para obter informações sobre como configurar o registro de auditoria, consulteHabilitando o registro de auditoria.

As seções a seguir descrevem os eventos de auditoria registrados pela Amazon WorkMail, quando os eventos são transmitidos e as informações sobre os campos do evento.

Registros de acesso à caixa de correio

Os eventos de acesso à caixa de correio fornecem informações sobre qual ação foi tomada (ou tentada) em qual objeto da caixa de correio. Um evento de acesso à caixa de correio é gerado para cada operação que você tenta executar em um item ou pasta em uma caixa de correio. Esses eventos são úteis para auditar o acesso aos dados da caixa de correio.

Campo	Descrição
event_timestamp	Quando o evento aconteceu, em milissegundos desde a época do Unix.
request_id	O ID que identifica a solicitação de forma exclusiva.
organization_arn	O ARN da & Amazon WorkMail Organization à qual o usuário autenticado pertence.

Campo	Descrição
user_id	O ID do usuário autenticado.
id_imitador	O ID do imitador. Presente somente se o recurso de representação tiver sido usado para a solicitação.
protocolo	O protocolo usado. O protocolo pode ser:`AutoDiscover` ,`EWS`,`IMAP`,`WindowsOutlook` ,`ActiveSync` ,`SMTP`,`WebMail`,`IncomingEmail` , ou`OutgoingEmail` .
source_ip	O endereço IP de origem da solicitação.
user_agent	O agente do usuário que fez a solicitação.
ação	A ação realizada no objeto, que pode 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`, ou`copy_to`.
owner_id	O ID do usuário proprietário do objeto que está sendo usado.
object_type	O tipo de objeto, que pode ser: Pasta, Mensagem ou Anexo.
item_id	O ID que identifica de forma exclusiva a mensagem que é o assunto do evento ou que contém o anexo que é o assunto do evento.

Campo	Descrição
caminho_da_pasta	O caminho da pasta que está sendo acionada ou o caminho da pasta que contém o item que está sendo acionado.
id_da_pasta	O ID que identifica de forma exclusiva a pasta que é o assunto do evento ou contém o objeto que é o assunto do evento.
caminho_de_anexo	O caminho dos nomes de exibição até o anexo afetado.
ação_permitida	Se a ação foi permitida. Pode ser verdadeiro ou falso.

Registros de controle de acesso

Eventos de controle de acesso são gerados sempre que uma regra de controle de acesso é avaliada. Esses registros são úteis para auditar acessos proibidos ou depurar configurações de controle de acesso.

Campo	Descrição
event_timestamp	Quando o evento aconteceu, em milissegundos desde a época do Unix.
request_id	O ID que identifica a solicitação de forma exclusiva.
organization_arn	O ARN da WorkMail organização à qual o usuário autenticado pertence.
user_id	O ID do usuário autenticado.
id_imitador	O ID do imitador. Presente somente se o recurso de representação tiver sido usado para a solicitação.

Campo	Descrição
protocolo	O protocolo usado, que pode ser: `AutoDiscover EWS`,`IMAP`,`WindowsOutlook` ,`ActiveSync` `c` ,`SMTP`,`WebMail`,`IncomingEmail` , ou`OutgoingEmail` .
source_ip	O endereço IP de origem da solicitação.
scope	O escopo da regra, que pode ser:`AccessControl` ,`DeviceAccessControl` , ou`ImpersonationAccessControl` .
id_de_regra	O ID da regra de controle de acesso correspondente. Quando não há regras correspondentes, rule_id não está disponível.
acesso_concedido	Se o acesso foi permitido. Pode ser verdadeiro ou falso.

Registros de autenticação

Os eventos de autenticação contêm informações sobre tentativas de autenticação.

> **Note**
>
> Os eventos de autenticação não são gerados para eventos de autenticação por meio do WorkMail WebMail aplicativo Amazon.

Campo	Descrição
event_timestamp	Quando o evento aconteceu, em milissegundos desde a época do Unix.

Campo	Descrição
request_id	O ID que identifica a solicitação de forma exclusiva.
organization_arn	O ARN da WorkMail organização à qual o usuário autenticado pertence.
user_id	O ID do usuário autenticado.
usuário	O nome de usuário com o qual a autenticação foi tentada.
protocolo	O protocolo usado, que pode ser: `AutoDiscover EWS`,`IMAP`,`WindowsOutlook` ,`ActiveSync` ,`SMTP`,`WebMail`,`IncomingEmail` , ou`OutgoingEmail` .
source_ip	O endereço IP de origem da solicitação.
user_agent	O agente do usuário que fez a solicitação.
method	O método de autenticação. Atualmente, somente o básico é suportado.
autentificação_bem-sucedida	Se a tentativa de autenticação foi bem-sucedida. Pode ser verdadeiro ou falso.
razão_falha_auth	O motivo da falha na autenticação. Presente somente se a autenticação falhar.

Registros do provedor de disponibilidade

Os eventos do provedor de disponibilidade são gerados para cada solicitação de disponibilidade WorkMail que a Amazon faz em seu nome ao seu provedor de disponibilidade configurado. Esses eventos são úteis para depurar a configuração do provedor de disponibilidade.

Campo	Descrição
event_timestamp	Quando o evento aconteceu, em milissegundos desde a época do Unix.
request_id	O ID que identifica a solicitação de forma exclusiva.
organization_arn	O ARN da WorkMail organização à qual o usuário autenticado pertence.
user_id	O ID do usuário autenticado.
type	O tipo de provedor de disponibilidade que está sendo chamado, que pode ser: `EWS` ou`LAMBDA`.
Domínio	O domínio para o qual a disponibilidade é obtida.
function_arn	O ARN do Lambda invocado, se o tipo for LAMBDA. Caso contrário, esse campo não estará presente.
ews_endpoint	O endpoint do EWS é do tipo EWS. Caso contrário, esse campo não estará presente.
error_message	A mensagem descrevendo a causa da falha. Se a solicitação for bem-sucedida, esse campo não estará presente.
evento_de_disponibilidade bem-sucedido	Se a solicitação de disponibilidade foi atendida com sucesso.

Usando o CloudWatch Insights com a Amazon WorkMail

Se você ativou o registro de eventos por e-mail no WorkMail console da Amazon ou habilitou a entrega de registros de auditoria para o CloudWatch Logs, você pode usar o Amazon CloudWatch Logs Insights para consultar seus registros de eventos. Para obter mais informações sobre como

habilitar o registro de eventos de e-mail em log, consulte Habilitando o registro de eventos de e-mail. Para obter mais informações sobre o CloudWatch Logs Insights, consulte Analisar dados de log com o CloudWatch Logs Insights no Guia do usuário do Amazon CloudWatch Logs.

Os exemplos a seguir demonstram como consultar CloudWatch registros para eventos de e-mail comuns. Você executa essas consultas no CloudWatch console. Para obter instruções sobre como executar essas consultas, consulte o Tutorial: Execute e modifique uma consulta de amostra no Guia do usuário do Amazon CloudWatch Logs.

Example Veja por que o usuário B não recebeu um e-mail enviado pelo usuário A.

O exemplo de código a seguir mostra como consultar um e-mail enviado pelo Usuário A ao Usuário B, classificados por carimbo de data e hora.

```
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/)
```

Essa ação retorna a mensagem enviada e ID de rastreamento. Use o ID de rastreamento no seguinte código de exemplo para consultar os registros de eventos para a mensagem enviada.

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

Retorna o ID de mensagem de e-mail e eventos de e-mail. `OUTGOING_EMAIL_SENT` indica que o e-mail foi enviado. `OUTGOING_EMAIL_BOUNCED` indica que o e-mail foi devolvido. Para ver se o e-mail foi recebido, consulte o ID da mensagem com o exemplo de código a seguir.

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

Essa ação também retorna a mensagem recebida, pois ela tem o mesmo ID de mensagem. Use o ID de rastreamento com o seguinte código de exemplo para consultar a entrega.

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

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

Isso retorna a ação de entrega e quaisquer ações de regra aplicáveis.

Example Veja todos os e-mails recebidos de um usuário ou domínio

O exemplo de código a seguir mostra como consultar todos os e-mails recebidos de um usuário específico.

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

O exemplo de código a seguir mostra como consultar todos os e-mails recebidos de um domínio específico.

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

Example Veja quem enviou e-mails devolvidos

O exemplo de código a seguir mostra como consultar e-mails enviados que foram devolvidos, e também retorna os motivos da devolução.

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

O exemplo de código a seguir demonstra como consultar e-mails recebidos que foram devolvidos. Ele também retorna os endereços de e-mail dos destinatários devolvidos e os motivos da devolução.

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

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

Example Veja quais domínios estão enviando spam

O exemplo de código a seguir mostra como consultar os destinatários da sua organização que estão recebendo spam.

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

O exemplo de código a seguir mostra como consultar o remetente dos e-mails de spam.

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

Example Veja por que um e-mail foi enviado para a pasta de spam do destinatário

O exemplo de código a seguir mostra como consultar e-mails identificados como spam, filtrados por objeto.

```
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"
```

Também é possível consultar pelo ID de rastreamento de e-mail para ver todos os eventos do e-mail.

Example Veja e-mails que correspondem às regras de fluxo de e-mail

O exemplo de código a seguir mostra como consultar e-mails que corresponderam às regras de fluxo de e-mails enviados.

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

O exemplo de código a seguir mostra como consultar e-mails recebidos que corresponderam às regras de fluxo de e-mails recebidos.

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

Example Veja quantos e-mails são recebidos ou enviados pela sua organização

O exemplo de código a seguir mostra como consultar o número de e-mails recebidos por cada destinatário na sua organização.

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

O exemplo de código a seguir mostra como consultar o número de e-mails enviados por cada remetente na sua organização.

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

Registrando chamadas de WorkMail API da Amazon com AWS CloudTrail

WorkMail A Amazon está integrada com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS service (Serviço da AWS) na Amazon WorkMail. CloudTrail captura todas as chamadas de API para a Amazon WorkMail como eventos, incluindo chamadas do WorkMail console da Amazon e de chamadas de código para as WorkMail APIs da Amazon. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para a Amazon. WorkMail Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à Amazon WorkMail, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais CloudTrail, consulte o Guia AWS CloudTrail do usuário.

WorkMail Informações da Amazon em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre na Amazon WorkMail, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo de eventos em sua AWS conta, incluindo eventos para a Amazon WorkMail, você deve criar uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as WorkMail ações da Amazon são registradas CloudTrail e documentadas na Amazon WorkMail API Reference. Por exemplo, chamadas para as operações de `CreateUser`, `CreateAlias`, e `GetRawMessageContent` API geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrailuserIdentity.

Entendendo as entradas do arquivo de WorkMail log da Amazon

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateUser` ação da WorkMail API da 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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateAlias` ação da WorkMail API da 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"
}
```


O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `GetRawMessageContent` ação da 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"
}
```

Habilitando o registro de eventos de e-mail

Você ativa o registro de eventos por e-mail no WorkMail console da Amazon para rastrear mensagens de e-mail da sua organização. O registro de eventos de e-mail usa uma função AWS Identity and Access Management vinculada ao serviço (SLR) para conceder permissões para publicar os registros de eventos de e-mail na Amazon. CloudWatch Para obter mais informações sobre funções vinculadas ao serviço do IAM, consulte Usar funções vinculadas ao serviço no Amazon WorkMail.

Nos registros de CloudWatch eventos, você pode usar ferramentas e métricas de CloudWatch pesquisa para rastrear mensagens e solucionar problemas de e-mail. Para obter mais informações sobre os registros de eventos que a Amazon WorkMail envia para CloudWatch, consulteMonitorando registros WorkMail de eventos de e-mail da Amazon. Para obter mais informações sobre CloudWatch registros, consulte o Guia do usuário do Amazon CloudWatch Logs.

Tópicos

- Ativar o registro em log de eventos de e-mail
- Criar um grupo de logs e um perfil do IAM personalizados para o registro em log de eventos de e-mail
- Desativar o registro em log de eventos de e-mail

- Prevenção contra o ataque “Confused deputy” entre serviços

Ativar o registro em log de eventos de e-mail

O seguinte ocorre quando você ativa o registro de eventos por e-mail usando as configurações padrão da Amazon WorkMail:

- Cria uma função AWS Identity and Access Management vinculada ao serviço —. `AmazonWorkMailEvents`
- Cria um grupo de CloudWatch registros —`/aws/workmail/emailevents/`*`organization-alias`*.
- Define a retenção de CloudWatch registros para 30 dias.

Como ativar o registro de eventos de e-mail em log

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a AWS região. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Configurações de registro.
4. Escolha a guia Configurações do registro de fluxo de e-mail.
5. Na seção Configurações do registro de fluxo de e-mail, escolha Editar.
6. Mova o controle deslizante Ativar eventos de e-mail para a posição ligado.
7. Execute um destes procedimentos:

   - (Recomendado) Escolha Usar configurações padrão.
   - (Opcional) Desmarque Usar as configurações padrão e selecione um Grupo de logs de destino e um Perfil do IAM da lista que for exibida.

> **Note**
>
> Escolha essa opção somente se você já criou um grupo de logs e um perfil do IAM personalizado usando a AWS CLI. Para ter mais informações, consulte Criar um grupo de logs e um perfil do IAM personalizados para o registro em log de eventos de e-mail.

8. Selecione Eu autorizo WorkMail a Amazon a publicar registros em minha conta usando essa configuração.
9. Selecione Salvar.

Criar um grupo de logs e um perfil do IAM personalizados para o registro em log de eventos de e-mail

Recomendamos usar as configurações padrão ao ativar o registro de eventos por e-mail para a Amazon WorkMail. Se você precisar de uma configuração de monitoramento personalizada, poderá usar o AWS CLI para criar um grupo de registros dedicado e uma função personalizada do IAM para o registro de eventos de e-mail.

Para criar um grupo de logs e um perfil do IAM personalizados para o registro em log de eventos de e-mail

1. Use o AWS CLI comando a seguir para criar um grupo de registros na mesma AWS região da sua WorkMail organização Amazon. Para obter mais informações, consulte create-log-groupna Referência de AWS CLI Comandos.

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

2. Crie um arquivo contendo a seguinte política:

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

```
    }
  ]
}
```

3. Use o AWS CLI comando a seguir para criar uma função do IAM e anexar esse arquivo como documento de política da função. Para obter mais informações, consulte create-role na Referência de comandos da AWS CLI .

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

> **Note**
>
> Se você for um usuário de política `WorkMailFullAccess` gerenciada, deverá incluir o termo `workmail` no nome da função. Essa política gerenciada somente permite configurar registros de eventos de e-mail usando funções com `workmail` no nome. Para obter mais informações, consulte Conceder permissões a um usuário para passar uma função para um AWS serviço no Guia do usuário do IAM.

4. Crie um arquivo contendo a política para a função do IAM que você criou na etapa anterior. No mínimo, a política deve conceder permissões à função para criar fluxos de log e colocar eventos no grupo de logs criado na etapa 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. Use o AWS CLI comando a seguir para anexar o arquivo de política à função do IAM. Para obter mais informações, consulte put-role-policyna Referência de AWS CLI Comandos.

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

Desativar o registro em log de eventos de e-mail

Desative o registro de eventos por e-mail no WorkMail console da Amazon. Se você não precisar mais usar o registro de eventos de e-mail, recomendamos que você exclua também o grupo de CloudWatch registros relacionado e a função vinculada ao serviço. Para ter mais informações, consulte Excluir uma função vinculada ao serviço no Amazon WorkMail.

Para desativar o registro de eventos de e-mail

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a AWS região. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Monitoring (Monitoramento).
4. Na seção Configurações de log, escolha Editar.
5. Mova o controle deslizante Habilitar eventos de e-mail para a posição desativado.
6. Selecione Salvar.

Prevenção contra o ataque “Confused deputy” entre serviços

O problema “confused deputy” é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado).

O serviço de chamadas pode ser manipulado para usar suas permissões para agir sobre os recursos de outro cliente que, de outra forma, ele não teria permissão para acessar.

Para evitar isso, AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com diretores de serviços que receberam acesso aos recursos em sua conta.

Recomendamos usar as `aws:SourceArn`chaves de contexto de condição `aws:SourceAccount`global nas políticas de recursos para limitar as permissões que a CloudWatch Logs e o Amazon S3 concedem aos serviços que estão gerando registros. Se você usar as duas chaves de contexto de condição global, os valores deverão usar o mesmo ID de conta quando usados na mesma declaração de política.

Os valores de `aws:SourceArn` devem ser os ARNs das fontes de entrega que estão gerando logs.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave da condição de contexto global `aws:SourceArn` com curingas (`*`) para as partes desconhecidas do ARN.

Habilitando o registro de auditoria

Você pode usar registros de auditoria para capturar informações detalhadas sobre o uso da sua WorkMail organização na Amazon. Os registros de auditoria podem ser usados para monitorar o acesso do usuário às caixas de correio, auditar atividades suspeitas e depurar as configurações do provedor de disponibilidade e controle de acesso.

> **Note**
>
> A política AmazonWorkMailFullAccessgerenciada não inclui todas as permissões necessárias para gerenciar entregas de registros. Se você estiver usando essa política para gerenciar WorkMail, certifique-se de que o principal (por exemplo, a função assumida) usado para configurar as entregas de registros também tenha todas as permissões necessárias.

A Amazon WorkMail oferece suporte a três destinos de entrega para registros de auditoria: CloudWatch Logs, Amazon S3 e Amazon Data Firehose. Para obter mais informações, consulte Registros que exigem permissões adicionais [V2] no Guia do usuário do Amazon CloudWatch Logs.

Além das permissões listadas em Logging que exigem permissões adicionais [V2], a Amazon WorkMail exige uma permissão adicional para configurar a entrega de registros:`workmail:AllowVendedLogDeliveryForResource`.

A entrega de um registro de trabalho consiste em três elementos:

- DeliverySource, um objeto lógico que representa o recurso ou recursos que enviam os registros. Para a Amazon WorkMail, é a Amazon WorkMail Organization.
- A DeliveryDestination, que é um objeto lógico que representa o destino real da entrega.
- Uma entrega, que conecta uma fonte de entrega ao destino da entrega.

Para configurar a entrega de registros entre a Amazon WorkMail e um destino, você pode fazer o seguinte:

- Crie uma fonte de entrega com PutDeliverySource.
- Crie um destino de entrega com PutDeliveryDestination.
- Se você estiver entregando registros entre contas, deverá usá-los PutDeliveryDestinationPolicyna conta de destino para atribuir uma política do IAM ao destino. Essa política autoriza a criação de uma entrega da fonte de entrega na conta A para o destino da entrega na conta B.
- Crie uma entrega combinando exatamente uma fonte de entrega e um destino de entrega usando CreateDelivery.

As seções a seguir fornecem os detalhes das permissões que você deve ter quando está conectado para configurar a entrega de registros para cada tipo de destino. Essas permissões podem ser concedidas a uma função do IAM com a qual você está conectado.

> **Important**
>
> É sua responsabilidade remover os recursos de entrega de registros após excluir o recurso gerador de registros.

Para remover os recursos de entrega de registros após excluir o recurso gerador de registros, siga estas etapas.

1. Exclua a entrega usando a DeleteDeliveryoperação.
2. Exclua o DeliverySourceusando a DeleteDeliverySourceoperação.
3. Se o DeliveryDestinationassociado ao DeliverySourceque você acabou de excluir for usado somente para esse específico DeliverySource, você poderá removê-lo usando a DeleteDeliveryDestinationsoperação.

Configurando o registro de auditoria usando o console da Amazon WorkMail

Você pode configurar o registro de auditoria no WorkMail console da Amazon:

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a AWS região. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e selecione uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Configurações de registro.
4. Escolha a guia Configurações do registro de auditoria.
5. Configure as entregas para o tipo de registro necessário usando o widget apropriado.
6. Selecione Salvar.

Registros enviados para CloudWatch Logs

Permissões de usuário

Para ativar o envio de CloudWatch registros para o Logs, você precisa estar conectado com as seguintes permissões.

```
{
    "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 do grupo de logs

O grupo de logs para o qual os logs estão sendo enviados deve ter uma política de recursos que contenha determinadas permissões. Se o grupo de registros atualmente não tiver uma política de recursos e o usuário que configura o registro tiver as `logs:DescribeLogGroups` permissões`logs:PutResourcePolicy`,`logs:DescribeResourcePolicies`, e para o grupo de registros, AWS criará automaticamente a política a seguir quando você começar a enviar os CloudWatch registros para o Logs.

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

```
}
```

Considerações sobre o limite do tamanho da política de recursos do grupo de logs

Esses serviços devem listar cada grupo de registros para o qual estão enviando registros na política de recursos. CloudWatch As políticas de recursos de registros estão limitadas a 5.120 caracteres. Um serviço que envia registros para um grande número de grupos de registros pode atingir esse limite.

Para mitigar isso, o CloudWatch Logs monitora o tamanho das políticas de recursos usadas pelo serviço que está enviando registros. Quando detecta que uma política se aproxima do limite de tamanho de 5.120 caracteres, o CloudWatch Logs ativa automaticamente a política `/aws/vendedlogs/*` de recursos desse serviço. Depois, você pode começar a usar grupos de logs com nomes que começam com `/aws/vendedlogs/` como destinos para os logs desses serviços.

Logs enviados ao Amazon S3

Permissões de usuário

Para permitir o envio de logs ao Amazon S3, é necessário fazer login com as permissões a seguir.

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

O bucket do S3 para o qual os logs estão sendo enviados deve ter uma política de recursos que contenha determinadas permissões. Se o bucket atualmente não tiver uma política de recursos e o usuário que configura o registro tiver as `S3:PutBucketPolicy` permissões `S3:GetBucketPolicy` e para o bucket, criará AWS automaticamente a seguinte política para ele quando você começar a enviar os registros para o 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:*"
```

```
                    ]
                }
            }
        }
    ]
}
```

Na política anterior, foraws:SourceAccount, especifique a lista de IDs de conta para os quais os registros estão sendo entregues a esse bucket. Para aws:SourceArn, especifique a lista de ARNs do recurso que gera os logs, no formulário arn:aws:logs:*source-region*:*source-account-id*:*.

Se o intervalo tiver uma política de recursos, mas essa política não contiver a declaração mostrada na política anterior, e o usuário que estiver configurando o registro tiver as S3:PutBucketPolicy permissões S3:GetBucketPolicy e para o intervalo, essa declaração será anexada à política de recursos do intervalo.

> **Note**
>
> Em alguns casos, você pode ver AccessDenied erros AWS CloudTrail se a s3:ListBucket permissão não tiver sido concedidadelivery.logs.amazonaws.com. Para evitar esses erros em seus CloudTrail registros, você deve conceder a s3:ListBucket permissão paradelivery.logs.amazonaws.com. Você também deve incluir os Condition parâmetros mostrados com o conjunto de s3:GetBucketAcl permissões na política de bucket anterior. Para simplificar isso, em vez de criar um novoStatement, você pode atualizar diretamente o AWSLogDeliveryAclCheck to be“Action”: [“s3:GetBucketAcl”, “s3:ListBucket”].

Criptografia no lado do servidor de bucket do Amazon S3

Você pode proteger os dados em seu bucket do Amazon S3 habilitando a criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou a criptografia do lado do servidor com uma chave armazenada em (SSE-KMS). AWS KMS AWS Key Management Service Para obter mais informações, consulte Proteger dados usando a criptografia no lado do servidor.

Se você escolher SSE-S3, nenhuma configuração adicional será necessária. O Amazon S3 lida com a chave de criptografia.

> **Warning**
>
> Se você escolher o SSE-KMS, deverá usar uma chave gerenciada pelo cliente, pois o uso de um Chave gerenciada pela AWS não é suportado nesse cenário. Se você configurar a criptografia usando uma chave AWS gerenciada, os registros serão entregues em um formato ilegível.

Ao usar uma AWS KMS chave gerenciada pelo cliente, você pode especificar o Amazon Resource Name (ARN) da chave gerenciada pelo cliente ao ativar a criptografia do bucket. Adicione o seguinte à política de chaves da chave gerenciada pelo cliente (não à política de bucket do S3), para que a conta de entrega de log possa gravar no bucket do S3.

Se você escolher o SSE-KMS, deverá usar uma chave gerenciada pelo cliente, pois o uso de uma chave AWS gerenciada não é suportado nesse cenário. Ao usar uma AWS KMS chave gerenciada pelo cliente, você pode especificar o Amazon Resource Name (ARN) da chave gerenciada pelo cliente ao ativar a criptografia do bucket. Adicione o seguinte à política de chaves da chave gerenciada pelo cliente (não à política de bucket do S3), para que a conta de entrega de log possa gravar no bucket do 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 `aws:SourceAccount`, especifique a lista de IDs de conta para os quais os registros estão sendo entregues a esse bucket. Para `aws:SourceArn`, especifique a lista de ARNs do recurso que gera os logs, no formulário `arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`.

Registros enviados para o Firehose

Permissões de usuário

Para ativar o envio de registros para o Firehose, você deve estar conectado com as seguintes permissões.

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

```
}
```

Perfis do IAM usados para permissões de recursos

Como o Firehose não usa políticas de recursos, AWS usa funções do IAM ao configurar esses registros para serem enviados ao Firehose. AWS cria uma função vinculada ao serviço chamada. AWSServiceRoleForLogDelivery Essa função vinculada ao serviço inclui as permissões a seguir.

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

Essa função vinculada ao serviço concede permissão para todos os streams de entrega do Firehose que têm a tag definida como. `LogDeliveryEnabled` `true` AWS fornece essa tag ao stream de entrega de destino quando você configura o registro.

Essa função vinculada ao serviço também tem uma política de confiança que permite que a entidade de serviço `delivery.logs.amazonaws.com` assuma a função vinculada ao serviço necessária. Essa política de confiança é a seguinte:

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

```
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Permissões específicas do console

Além das permissões listadas nas seções anteriores, se você estiver configurando a entrega de registros usando o console em vez das APIs, também precisará das seguintes permissões:

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

Validação de conformidade para a Amazon WorkMail

Auditores terceirizados avaliam a segurança e a conformidade da Amazon WorkMail como parte de vários programas de AWS conformidade. Isso inclui SOC, ISO e C5.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte AWS Services in Scope by Compliance Program. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Fazer download dos relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar a Amazon WorkMail é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentos aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos focados em segurança e conformidade em. AWS
- AWS Recursos de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Config— Esse AWS serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência na Amazon WorkMail

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, a Amazon WorkMail oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Segurança da infraestrutura na Amazon WorkMail

> **Note**
>
> A Amazon WorkMail interrompeu o suporte para Transport Layer Security (TLS) 1.0 e 1.1. Se você estiver usando o TLS 1.0 ou 1.1, deverá atualizar a versão do TLS para 1.2. Para obter mais informações, consulte TLS 1.2 para se tornar o nível mínimo do protocolo TLS para todos os endpoints da API da AWS.

Como um serviço gerenciado, a Amazon WorkMail é protegida pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar a Amazon WorkMail pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Começando com a Amazon WorkMail

Depois de concluir oPré-requisitos, você estará pronto para começar a usar a Amazon WorkMail. Para ter mais informações, consulte Começando com a Amazon WorkMail.

Você pode aprender mais sobre a migração de caixas de correio existentes para a Amazon WorkMail, a interoperabilidade com o Microsoft Exchange e as cotas da WorkMail Amazon nas seções a seguir.

Tópicos

Começando com a Amazon WorkMail

Se você é um novo WorkMail usuário da Amazon ou um usuário existente da Amazon WorkDocs ou da Amazon WorkSpaces, comece a usar a Amazon WorkMail concluindo as etapas a seguir.

> **Note**
>
> Conclua os Pré-requisitos antes de começar a usar.

Tópicos

Etapa 1: Faça login no WorkMail console da Amazon

Você deve entrar no WorkMail console da Amazon antes de poder adicionar usuários e gerenciar suas contas e caixas de correio.

Para fazer login no WorkMail console da Amazon

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.
2. Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações sobre as regiões, consulte Regiões e Endpoints em Referência geral da Amazon Web Services.

Etapa 2: configurar seu WorkMail site da Amazon

1. Depois de entrar no WorkMail console da Amazon, você configura sua organização e adiciona um domínio. Recomendamos usar um domínio dedicado para sua WorkMail organização Amazon. Para obter mais informações, consulte Adicionar um domínio e Criar uma organização.
2. (Opcional) Você pode optar por usar um domínio de teste gratuito fornecido pela Amazon WorkMail. Se você optar por fazer isso, vá para a etapa 4.

   > **Note**
   >
   > Os domínios de teste usam esse formato: *alias*.awsapps.com. À medida que avança, lembre-se de que você só deve usar domínios de teste para testes. Não use um domínio de teste para um ambiente de produção. Além disso, você deve ter pelo menos um usuário habilitado na sua WorkMail organização Amazon. Se você não tiver um usuário habilitado, o domínio poderá ficar disponível para registro e uso por outros clientes.

3. Se você usa um domínio externo, verifique esse domínio adicionando os registros apropriados de texto (TXT) e troca de mensagens (MX) ao seu serviço de Sistema de Nomes de Domínio (DNS). Os registros TXT permitem que você insira notas no DNS. Os registros MX especificam

os servidores de e-mail de entrada. Certifique-se de definir seu domínio como padrão para sua organização. Para obter mais informações, consulte Escolher o domínio padrão e Verificar domínios.

4. Crie novos usuários ou habilite seus usuários de diretório existentes para a Amazon WorkMail. Para ter mais informações, consulte Incluir um usuário.
5. (Opcional) Se você já tiver caixas de correio do Microsoft Exchange, migre-as para a Amazon. WorkMail Para ter mais informações, consulte Migração para a Amazon WorkMail.

Depois de concluir a configuração do seu WorkMail site da Amazon, você pode acessar a Amazon WorkMail usando a URL do aplicativo web.

Para localizar o URL do seu aplicativo WorkMail web da Amazon

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Para fazer isso, abra a lista Selecionar uma região, localizada à direita da caixa de pesquisa, e escolha a região desejada. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizações e, em seguida, selecione o nome da organização.

   A página Configurações da organização é exibida e mostra a URL em Login do usuário. As URLs têm o seguinte formato: https://*alias*.awsapps.com/mail.

Etapa 3: configurar o acesso WorkMail do usuário da Amazon

Escolha entre as seguintes opções para configurar o acesso WorkMail do usuário da Amazon:

- Configurar o acesso dos usuários em um cliente de desktop existente usando o cliente do Microsoft Outlook. Para obter mais informações, consulte Connect Microsoft Outlook à sua WorkMail conta da Amazon.
- Configurar o acesso de usuário em um dispositivo móvel, como Kindle, Android, iPad ou iPhone. Para obter mais informações, consulte Conceitos básicos ao usar um dispositivo móvel.
- Para configurar o acesso de usuário, use qualquer software cliente compatível com o protocolo IMAP (Internet Mail Access Protocol). Para obter mais informações, consulte Conectar clientes IMAP à sua WorkMail conta Amazon.

Mais atributos

- Migração para a Amazon WorkMail
- Interoperabilidade entre Amazon e WorkMail Microsoft Exchange
- WorkMail Cotas da Amazon

Migração para a Amazon WorkMail

Você pode migrar para a Amazon WorkMail do Microsoft Exchange, do Microsoft Office 365, do G Suite Basic (antigo Google Apps for Work) e de outras plataformas trabalhando com um de nossos parceiros. Para obter mais informações sobre nossos parceiros, consulte Amazon WorkMail Features.

Tópicos

- Etapa 1: criar ou habilitar usuários na Amazon WorkMail
- Etapa 2: migrar para a Amazon WorkMail
- Etapa 3: Concluir a migração para a Amazon WorkMail

Etapa 1: criar ou habilitar usuários na Amazon WorkMail

Antes de migrar seus usuários, você deve adicionar esses usuários na Amazon WorkMail para provisionar suas caixas de correio. Para ter mais informações, consulte Incluir um usuário.

Etapa 2: migrar para a Amazon WorkMail

Você pode trabalhar com qualquer parceiro de AWS migração para migrar para a Amazon WorkMail. Para obter informações sobre esses provedores, consulte os WorkMailrecursos da Amazon.

Para migrar suas caixas de correio, crie um WorkMail usuário dedicado da Amazon para atuar como administrador de migração. O procedimento a seguir concede permissão a esse usuário para acessar todas as caixas de correio na organização.

Como criar um administrador de migração

1. Execute um destes procedimentos:

- No WorkMail console da Amazon, crie um novo usuário para atuar como administrador de migração. Para ter mais informações, consulte Incluir um usuário.
- No seu Active Directory, crie um novo usuário para atuar como administrador de migração e, em seguida, habilite o usuário para a Amazon WorkMail. Para ter mais informações, consulte Como habilitar usuários.

2. No painel de navegação do WorkMail console da Amazon, escolha Organizations e, em seguida, escolha o nome da sua organização.
3. Escolha Configurações da organização, escolha Migração e, em seguida, Editar.
4. Mova o controle deslizante Habilitado para migração para a posição ativado.
5. Abra o Administrador de migração e selecione um usuário.
6. Escolha Salvar.

Etapa 3: Concluir a migração para a Amazon WorkMail

Depois de migrar suas contas de e-mail para a Amazon WorkMail, você pode verificar seus registros DNS e configurar seus clientes de desktop e dispositivos móveis.

Para concluir a migração para a Amazon WorkMail

1. Verifique se todos os registros DNS estão atualizados e se apontam para a Amazon WorkMail. Para obter mais informações sobre os registros DNS necessários, consulte Adicionar um domínio.

   > **Note**
   >
   > O processo de atualização de registros DNS pode levar várias horas. Se um novo item for exibido em uma caixa de correio de origem enquanto os registros MX estiverem sendo alterados, execute a ferramenta de migração novamente para migrar os novos itens após os registros DNS terem sido atualizados.

2. Para obter mais informações sobre como configurar seus clientes de desktop ou dispositivos móveis para usar a Amazon WorkMail, consulte Conecte o Microsoft Outlook à sua WorkMail conta da Amazon no Guia do WorkMail Usuário da Amazon.

Interoperabilidade entre Amazon e WorkMail Microsoft Exchange

A interoperabilidade entre a Amazon e o WorkMail Microsoft Exchange Server permite que você minimize as interrupções para seus usuários ao migrar caixas de correio para a Amazon WorkMail ou usar a Amazon WorkMail para um subconjunto de suas caixas de correio corporativas.

Essa interoperabilidade permite que você use o mesmo domínio corporativo para caixas de correio nos dois ambientes. Dessa forma, os usuários podem agendar reuniões com compartilhamento bidirecional de informações de disponibilidade do calendário.

Pré-requisitos

Antes de habilitar a interoperabilidade com o Microsoft Exchange, proceda da seguinte maneira:

- Verifique se você tem pelo menos um usuário habilitado para a Amazon. WorkMail Isso é necessário para definir as configurações de disponibilidade do Microsoft Exchange. Para habilitar um usuário, siga as etapas em Habilitar o roteamento de e-mails para um usuário.
- Configure um Active Directory (AD) Connector. A configuração de um AD Connector com o diretório on-premises permite que os usuários continuem usando as credenciais corporativas existentes. Para obter mais informações, consulte Criar um AD Connector e integrar a Amazon WorkMail com seu diretório local.
- Configure sua WorkMail organização na Amazon. Crie uma WorkMail organização da Amazon que use o AD Connector que você configurou.
- Adicione seus domínios corporativos à sua WorkMail organização da Amazon e, em seguida, verifique-os no WorkMail console da Amazon. Caso contrário, os e-mails enviados a esse alias serão devolvidos. Para obter mais informações, consulte Trabalhar com domínios.
- Migre caixas de correio para a Amazon WorkMail. Permita que os usuários provisionem e migrem caixas de correio do seu ambiente local para a Amazon. WorkMail Para obter mais informações, consulte Habilitar usuários existentes e consulte Migração para a Amazon WorkMail.

  > **Note**
  >
  > Não atualize os registros DNS para apontar para a Amazon WorkMail. Isso garante que o Microsoft Exchange permaneça como o servidor primário para e-mails recebidos pelo tempo que você desejar a interoperabilidade entre os dois ambientes.

- Certifique-se de que os nomes principais do usuário (UPNs) no Active Directory seja correspondentes aos endereços SMTP principais deles.

A Amazon WorkMail faz solicitações HTTPS para a URL do Exchange Web Services (EWS) no Microsoft Exchange para obter informações de disponibilidade e disponibilidade do calendário.

Para provedores de disponibilidade baseados em EWS, a Amazon WorkMail faz solicitações HTTPS para a URL do Exchange Web Services (EWS) no Microsoft Exchange para obter informações de disponibilidade e disponibilidade do calendário. Portanto, os pré-requisitos a seguir se aplicam somente aos provedores de disponibilidade baseados no EWS.

- Certifique-se de que as configurações relevantes do firewall estejam definidas para permitir o acesso da Internet. A porta padrão das solicitações HTTPS é 443.
- A Amazon só WorkMail pode fazer solicitações HTTPS bem-sucedidas para a URL do EWS no Microsoft Exchange quando um certificado assinado por uma autoridade de certificação (CA) válida está disponível em seu ambiente Microsoft Exchange. Para obter mais informações, consulte Criar uma solicitação de certificado do Exchange Server para uma autoridade de certificação no site de documentação do Microsoft Exchange.
- Você precisa habilitar a Autenticação básica para o EWS no Microsoft Exchange. Para obter mais informações, consulte Virtual Directories: Exchange 2013 no blog do programa de recompensas do Microsoft MVP.

Adicionar domínios e habilitar caixas de correio

Adicione seus domínios corporativos à Amazon WorkMail para que eles possam ser usados em endereços de e-mail. Certifique-se de que os domínios adicionados à Amazon WorkMail sejam verificados e, em seguida, permita que usuários e grupos provisionem caixas de correio na Amazon. WorkMail Os recursos não podem ser habilitados na Amazon WorkMail enquanto estão no modo de interoperabilidade e devem ser recriados na Amazon WorkMail depois que você desabilitar o modo de interoperabilidade. No entanto, é possível usá-los para agendar reuniões durante o modo de interoperabilidade. Os recursos do Microsoft Exchange são sempre mostrados na guia Usuários na Amazon WorkMail.

- Para obter mais informações, consulte Adicionar domínios, Habilitar usuários existentes e Habilitar um grupo existente.

> **Note**
>
> Para garantir a interoperabilidade com o Microsoft Exchange, não atualize os registros DNS para apontar para os registros da Amazon. WorkMail O Microsoft Exchange continuará sendo o servidor primário para e-mails recebidos pelo tempo que você desejar ter interoperabilidade entre os dois ambientes.

Habilitar a interoperabilidade

Se você não criou uma WorkMail organização na Amazon, você pode usar a API pública para criar uma nova WorkMail organização com o modo de interoperabilidade ativado.

Se você já tem uma WorkMail organização da Amazon com um AD Connector vinculado ao Active Directory e também tem o Microsoft Exchange, entre em contato com o AWS Support para obter ajuda para habilitar a interoperabilidade do Microsoft Exchange para uma organização Amazon WorkMail existente.

Crie contas de serviço no Microsoft Exchange e na Amazon WorkMail

> **Note**
>
> Não é necessário criar uma conta de serviço no Exchange quando o Exchange não é usado como back-end para um provedor de disponibilidade personalizado.

Para acessar as informações de disponibilidade e disponibilidade do calendário, crie uma conta de serviço no Microsoft Exchange e na Amazon. WorkMail A conta de serviço do Microsoft Exchange é qualquer usuário do Microsoft Exchange que tenha acesso às informações de disponibilidade do calendário de outros usuários do Exchange. O acesso é concedido por padrão, portanto, permissões especiais não são necessárias.

Da mesma forma, a conta WorkMail de serviço da Amazon é qualquer usuário na Amazon WorkMail que tenha acesso às informações de disponibilidade e disponibilidade do calendário de outros usuários da Amazon WorkMail . Isso também é concedido por padrão. Você deve criar o WorkMail usuário da Amazon em seu diretório local e, em seguida WorkMail, habilitar esse usuário para a Amazon integrar a Amazon WorkMail com o AD Connector em seu diretório.

Limitações no modo de interoperabilidade

Quando sua organização estiver no modo de interoperabilidade, o gerenciamento de qualquer usuário, grupo e recurso deve ser realizado usando o Centro de administração do Exchange. Para habilitar WorkMail usuários e grupos da Amazon, use AWS Management Console o. Para obter mais informações, consulte Habilitar usuários existentes e Habilitar um grupo existente.

Ao habilitar um usuário ou grupo para a Amazon WorkMail, você não pode editar os endereços de e-mail ou aliases desses usuários e grupos. Eles também devem ser configurados por meio do Centro de administração do Exchange. A Amazon WorkMail sincroniza as alterações em seu diretório a cada quatro horas.

Os recursos não podem ser criados ou habilitados na Amazon WorkMail enquanto estão no modo de interoperabilidade. No entanto, todos os seus recursos do Exchange estão disponíveis no catálogo de WorkMail endereços da Amazon e podem ser usados para agendar reuniões normalmente.

Defina as configurações de disponibilidade na Amazon WorkMail

Defina as configurações de disponibilidade na Amazon WorkMail para permitir a consulta de sistemas externos, oferecer funcionalidade de calendário e obter informações de disponibilidade e disponibilidade do calendário. A Amazon WorkMail oferece suporte a dois modos de obtenção de informações de disponibilidade a partir de um sistema remoto:

- Exchange Web Services (EWS) — Nessa configuração, a Amazon WorkMail consultará um servidor Exchange ou outra WorkMail organização para obter informações de disponibilidade usando o protocolo EWS. Essa é a configuração mais simples, mas exige que o endpoint EWS do servidor Exchange seja acessível pela internet pública.
- Provedor de disponibilidade personalizado (CAP) — Nessa configuração, um administrador pode configurar uma função do AWS Lambda para obter informações de disponibilidade do usuário para um determinado domínio de e-mail. Dependendo da plataforma do seu servidor de e-mail, o uso do CAP com a Amazon WorkMail oferece os seguintes benefícios:
  - Obtenha a disponibilidade do usuário no EWS interno sem a necessidade de abrir o firewall para WorkMail.
  - Obter a disponibilidade dos usuários em sistemas que não sejam Exchange ou EWS, como o Google Workspace (anteriormente conhecido como G Suite).

Tópicos

Configurar um provedor de disponibilidade baseado em EWS

Para definir configurações de disponibilidade baseadas no EWS no console, conclua o procedimento a seguir:

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Para fazer isso, abra a lista Selecionar uma região, localizada à direita da caixa de pesquisa, e escolha a região desejada. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizações e, em seguida, escolha o nome de uma organização.
3. No painel de navegação, escolha Configurações da organização e, em seguida, escolha a guia Interoperabilidade.
4. Escolha Adicionar configuração de disponibilidade e, em seguida, insira as seguintes informações:

   - Tipo – Selecione EWS.
   - Domínio — O domínio para o qual WorkMail tentará consultar as informações de disponibilidade usando essa configuração.
   - URL do EWS — A Amazon WorkMail consultará esse URL no endpoint do EWS. Consulte a seção Como obter a URL do EWS deste guia.
   - Endereço de e-mail do usuário — O endereço de e-mail do usuário que WorkMail será usado para se autenticar no endpoint do EWS.
   - Senha — A senha que WorkMail será usada para se autenticar no endpoint do EWS.
5. Escolha Salvar.

Como obter a URL do EWS

Para obter a URL do EWS para o Exchange usando o Microsoft Outlook, conclua o procedimento a seguir:

1. Faça login no Microsoft Outlook no Windows para qualquer usuário do seu ambiente do Exchange.
2. Mantenha a tecla Ctrl pressionada e abra o menu de contexto (botão direito do mouse) no ícone do Microsoft Outlook na barra de tarefas.
3. Escolha Testar e-mail AutoConfiguration.
4. Insira o endereço de e-mail e a senha do usuário do Microsoft Exchange e escolha Test.
5. Na janela Results, copie o valor de Availability Service URL.

Para obter o URL do EWS para troca usando PowerShell, no PowerShell prompt, execute o seguinte comando:

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

Para obter o URL do EWS para a Amazon WorkMail, primeiro encontre o domínio do EWS em WorkMail endpoints e cotas da Amazon. Insira a URL do EWS `https://"EWS domain"/EWS/Exchange.asmx` e substitua "domínio do EWS" pelo seu domínio do EWS.

Para configurar um Provedor de disponibilidade personalizado

Para configurar um Provedor de disponibilidade personalizado (CAP), conclua o procedimento a seguir:

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Para fazer isso, abra a lista Selecionar uma região, localizada à direita da caixa de pesquisa, e escolha a região desejada.
2. No painel de navegação, escolha Organizações e, em seguida, escolha o nome de uma organização.
3. No painel de navegação, escolha Configurações da organização e, em seguida, interoperabilidade.
4. Escolha Adicionar configuração de disponibilidade e, em seguida, insira as seguintes informações:

   - Tipo – Selecione CAP Lambda.
   - Domínio — O domínio para o qual WorkMail tentará consultar as informações de disponibilidade usando essa configuração.
   - ARN – O ARN da função do Lambda que fornecerá as informações de disponibilidade.

Para criar uma função do CAP Lambda, consulte Para criar uma função do Lambda do Provedor de disponibilidade personalizada.

Para criar uma função do Lambda do Provedor de disponibilidade personalizada

Os Provedores de disponibilidade personalizados (CAPs) são configurados com um protocolo de solicitação e resposta baseado em JSON, escrito em um esquema JSON bem definido. Uma função do Lambda analisará a solicitação e fornecerá uma resposta válida.

Tópicos

- Elementos de solicitações e respostas
- Como conceder acesso ao
- Exemplo de Amazon WorkMail usando uma função CAP Lambda

Elementos de solicitações e respostas

Elementos da solicitação

Veja a seguir um exemplo de solicitação usada para configurar um CAP para um WorkMail usuário da 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"
    }
}
```

Uma solicitação é composta por três seções: solicitante, caixas de correio e janela. Elas são descritas nas seguintes seções Solicitante, Caixas de correio e Window deste guia.

Solicitante

A seção do solicitante fornece informações sobre o usuário que fez a solicitação original para a Amazon WorkMail. Os CAPs usam essas informações para mudar o comportamento do provedor. Por exemplo, esses dados podem ser usados para representar o mesmo usuário no provedor de disponibilidade de back-end ou certos detalhes podem ser omitidos da resposta.

Campo	Descrição	Obrigatório
`Email`	O endereço de e-mail principal do solicitante.	Sim
`Username`	O nome de usuário do solicitante.	Sim
`Organization`	O ID da organização do solicitante.	Sim
`UserID`	O ID do solicitante.	Sim
`Origin`	O endereço remoto do solicitante.	Não
`Bearer`	Reservado para uso futuro.	Não

Caixas de correio

A seção de caixas de correio contém uma lista separada por vírgulas dos endereços de e-mail dos usuários para os quais as informações de disponibilidade são solicitadas.

Window

A seção da janela contém a janela de tempo para a qual as informações de disponibilidade são solicitadas. Ambos `startDate` e `endDate` são especificados em UTC e são formatados de acordo com a RFC 3339. Não se espera que eventos sejam truncados. Em outras palavras, se um evento começar antes do `StartDate` definido, será usado o início original.

Elementos de resposta

A Amazon WorkMail aguardará 25 segundos para obter uma resposta da função CAP Lambda. Depois de 25 segundos, a Amazon WorkMail presumirá que a função falhou e gerará falhas para as caixas de correio associadas na resposta do EWS GetUserAvailability. Isso não fará com que toda a GetUserAvailability operação falhe.

Veja a seguir um exemplo de resposta da configuração definida no início desta seção:

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

Uma resposta é composta por uma única seção de caixas de correio que consiste em uma lista de caixas de correio. Cada caixa de correio para a qual a disponibilidade é obtida com sucesso é composta por três seções: caixa de correio, eventos e workingHours. Se o provedor de disponibilidade não conseguiu obter as informações de disponibilidade de uma caixa de correio, a seção será composta por duas seções: caixa de correio e erro. Elas são descritas nas seguintes seções Caixa de correio, Eventos, Horário de trabalho, Fuso horário, Períodos de trabalho e Erro deste guia.

Caixa de correio

A seção caixa de correio é o endereço de e-mail do usuário encontrado na seção caixas de correio da solicitação.

Eventos

A seção eventos é uma lista de eventos que ocorrem na janela solicitada. Cada evento é definido com os seguintes parâmetros:

Campo	Descrição	Obrigatório
`startTime`	A hora de início do evento em UTC e formatada de acordo com a RFC3339.	Sim

Campo	Descrição	Obrigatório
`endTime`	A hora de término do evento em UTC e formatada de acordo com a RFC3339.	Sim
`busyType`	O tipo de disponibilidade do evento. Pode ser `Busy`, `Free`, ou `Tentative` .	Sim
`details`	Os detalhes do evento.	Não
`details.subject`	O tema do evento.	Sim
`details.location`	A localização do evento.	Sim
`details.instanceType`	O tipo de instância do evento. Pode ser `Single_Instance` , `Recurring_Instance` , ou `Exception` .	Sim
`details.isMeeting`	Um booleano para indicar se o evento tem participantes.	Sim
`details.isReminderSet`	Um booleano para indicar se o evento tem definição de lembretes.	Sim
`details.isPrivate`	Um booleano para indicar se o evento está definido como privado.	Sim

Horário de trabalho

A seção Horas de trabalho contém informações sobre o horário de trabalho do proprietário da caixa de correio. Ele contém duas seções: fuso horário e Períodos de trabalho.

Fuso horário

A subseção fuso horário descreve o fuso horário do proprietário da caixa de correio. É importante renderizar corretamente o horário de trabalho do usuário quando o solicitante trabalha em um fuso horário diferente. O provedor de disponibilidade precisa descrever explicitamente o fuso horário, em vez de usar um nome. Usar a descrição padronizada do fuso horário ajuda a evitar incompatibilidades de fuso horário.

Campo	Descrição	Obrigatório
`name`	O nome do fuso horário.	Sim
`bias`	O deslocamento padrão do GMT em minutos.	Sim
`standardTime`	O início do horário padrão para o fuso horário especific ado.	Não
`daylightTime`	O início do horário de verão para o fuso horário especific ado.	Não

Você deve definir ou omitir ambos `standardTime` e `daylightTime`. Os campos nos objetos `standardTime` e `daylightTime` são:

Campo	Descrição	Valores permitidos
`offset`	O deslocamento em relação ao deslocamento padrão em minutos.	N/D
`time`	O horário em que ocorre a transição entre o horário padrão e o horário de verão, especificado como `hh:mm:ss`.	N/D

Campo	Descrição	Valores permitidos
`month`	O mês em que ocorre a transição entre o horário padrão e o horário de verão.	`JAN`,`FEB`, `MAR`, `APR`, `JUN`, `JUL`, `AUG`, `SEP`, `OCT`, `NOV`, `DEC`
`week`	A semana do mês específico em que ocorre a transição entre o horário padrão e o horário de verão.	`FIRST`, `SECOND`, `THIRD`, `FOURTH`, `LAST`
`dayOfWeek`	O dia da semana específica em que ocorre a transição entre o horário padrão e o horário de verão.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Períodos de trabalho

A seção Períodos de trabalho contém um ou mais objetos de período de trabalho. Cada período define o início e o fim do dia de trabalho para um ou mais dias.

Campo	Descrição	Valores permitidos
`startMinutes`	O início do dia de trabalho em minutos a partir da meia-noite.	N/D
`endMinutes`	O fim do dia de trabalho em minutos a partir da meia-noite.	N/D
`days`	Os dias aos quais esse período se aplica.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Erro

O campo erro pode conter mensagens de erro arbitrárias. A tabela a seguir lista um mapeamento de códigos conhecidos para códigos de erro do EWS. Todas as outras mensagens serão mapeadas para `ERROR_FREE_BUSY_GENERATION_FAILED`.

Valor	Código de erro 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	

Como conceder acesso ao

Execute o comando do Lambda a seguir a partir de AWS Command Line Interface (AWS CLI). Esse comando adiciona uma política de recursos à função do Lambda que analisa o CAP. Essa função permite que o serviço de WorkMail disponibilidade da Amazon invoque sua função 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
```

No comando, adicione os seguintes parâmetros onde indicado:

- *LAMBDA_REGION* – Nome da região em que o CAP Lambda é implantado. Por exemplo, `us-east-1`.
- *CAP_FUNCTION_NAME* – Nome da função do CAP Lambda.

> **Note**
>
> Isso pode ser o nome, o alias ou o ARN parcial ou completo da função do CAP Lambda.

- *WM_REGION – Nome da região* em que a WorkMail organização da Amazon invoca a função Lambda.

> **Note**
>
> Somente as regiões a seguir estão disponíveis para uso com CAP:
>
> - Leste dos EUA (Norte da Virgínia)
> - Oeste dos EUA (Oregon)
> - Europa (Irlanda)

- *WM_ACCOUNT_ID* – O ID da conta da organização.
- *ORGANIZATION_ID* – O ID de organização que invoca o CAP Lambda. Por exemplo, ID de organização: m-934ebb9eb57145d0a6cab566ca81a21f.

> **Note**
>
> *LAMBDA_REGION* e *WM_REGION* serão diferentes somente se forem necessárias chamadas entre regiões. Se as chamadas entre regiões não forem necessárias, elas serão iguais.

Exemplo de Amazon WorkMail usando uma função CAP Lambda

Para ver um exemplo da Amazon WorkMail usando uma função CAP Lambda para consultar um endpoint do EWS, consulte este AWSexemplo de aplicativo no repositório de aplicativos Serverless for Amazon. WorkMail GitHub

Definir as configurações de disponibilidade no Microsoft Exchange

Para redirecionar todas as solicitações de informações de disponibilidade ou disponibilidade do calendário para usuários habilitados para a Amazon WorkMail, configure um espaço de endereço de disponibilidade no Microsoft Exchange.

Use o PowerShell comando a seguir para criar o espaço de endereço:

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

No prompt, insira as credenciais da conta de WorkMail serviço da Amazon. O nome de usuário deve ser inserido como **domain\username** (ou seja, ***orgname*.awsapps.com\workmail_service_account_*username***). Aqui, ***orgname*** representa o nome da WorkMail organização Amazon. Para ter mais informações, consulte Crie contas de serviço no Microsoft Exchange e na Amazon WorkMail.

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

Para obter mais informações, consulte AvailabilityAddressSpaceAdd-on Microsoft Docs.

Habilite o roteamento de e-mail entre usuários do Microsoft Exchange e da Amazon WorkMail

Com o roteamento de e-mail entre o Microsoft Exchange Server e a Amazon WorkMail, os usuários podem manter seus endereços de e-mail existentes após migrarem para a Amazon. WorkMail O roteamento de e-mails permite que você mantenha o Microsoft Exchange Server como o servidor SMTP (Simple Mail Transfer Protocol) principal para e-mails recebidos em sua organização.

Antes de usar o roteamento de e-mails, é necessário concluir os pré-requisitos a seguir:

- Habilitar o modo de interoperabilidade para sua organização. Para ter mais informações, consulte Habilitar a interoperabilidade.
- Certifique-se de ver seu domínio no WorkMail console da Amazon.
- Verifique se o Microsoft Exchange Server pode enviar ei-mails para a Internet. Talvez seja necessário configurar um conector de envio. Para obter mais informações sobre conectores de envio, consulte Criar um conector de envio no Exchange Server para enviar e-mails para a Internet na documentação da Microsoft.

Habilitar o roteamento de e-mails para um usuário

Recomendamos que você primeiro conclua as etapas a seguir para testar usuários antes de aplicar alterações à sua organização.

1. Ative a conta de usuário que você está migrando para a Amazon WorkMail. Para obter mais informações, consulte Habilitar usuários existentes.
2. No WorkMail console da Amazon, verifique se há pelo menos dois endereços de e-mail associados ao usuário habilitado.
   - <*workmailuser*@*orgname*.awsapps.com> (esse é adicionado automaticamente e pode ser usado para testes sem o Microsoft Exchange.)
   - <*workmailuser*@*yourdomain*.com> (esse é adicionado automaticamente e é o endereço principal do Microsoft Exchange.)

     Para obter mais informações, consulte Editar endereços de e-mail do usuário.
3. Certifique-se de migrar todos os dados da caixa de correio no Microsoft Exchange para a caixa de correio na Amazon. WorkMail Para obter mais informações, consulte Migração para a Amazon WorkMail.
4. Depois que todos os dados forem migrados, desabilite a caixa de correio do usuário no Microsoft Exchange. Em seguida, crie um usuário de e-mail (ou usuário habilitado para e-mail) que tenha o endereço SMTP externo apontado para a Amazon. WorkMail Para isso, use os comandos a seguir no Shell de gerenciamento do Exchange:

   > **Important**
   >
   > As etapas a seguir apagam o conteúdo da caixa de correio. Certifique-se de que seus dados tenham sido migrados para a Amazon WorkMail antes de tentar habilitar o roteamento de e-mail. Alguns clientes de e-mail não mudam facilmente para a Amazon WorkMail quando você executa esse comando. Para ter mais informações, consulte Configuração de cliente de e-mail.

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

```
Disable-Mailbox $old_mailbox
```

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

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

Nos comandos acima, *orgname* representa o nome da sua organização na Amazon WorkMail . Para obter mais informações, consulte Desabilitando a caixa de correio e Habilitando usuários de email na Microsoft. TechNet

5. Envie um e-mail de teste para o usuário (conforme o exemplo acima, **workmailuser@yourdomain.com**). Se o roteamento de e-mail tiver sido habilitado corretamente, o usuário deverá ser capaz de fazer login na WorkMail caixa de correio da Amazon e receber o e-mail.

> **Note**
>
> O Microsoft Exchange continuará sendo o servidor primário para e-mails recebidos durante a interoperabilidade entre os dois ambientes. Para garantir a interoperabilidade com o Microsoft Exchange, os registros DNS não devem ser atualizados para apontar para a Amazon WorkMail até mais tarde.

Definição pós-configuração

As etapas acima movem a caixa de correio de um usuário do Microsoft Exchange Server para a Amazon WorkMail, mantendo o usuário no Microsoft Exchange como um contato. Como o usuário migrado agora é um usuário de e-mail externo, o Microsoft Exchange Server impõe restrições adicionais. Pode haver ainda requisitos adicionais de configuração para concluir a migração.

- É possível que o usuário não consiga enviar e-mail para grupos por padrão. Para habilitar essa funcionalidade, é necessário adicionar o usuário a uma lista segura de remetentes para todos os grupos. Para obter mais informações, consulte Gerenciamento de entrega na Microsoft TechNet.
- Talvez o usuário não consiga reservar recursos. Para habilitar essa funcionalidade, defina as `ProcessExternalMeetingMessages` de todos os recursos que o usuário precisa acessar. Para obter mais informações, consulte Set- CalendarProcessing on Microsoft TechNet.

Configuração de cliente de e-mail

Alguns clientes de e-mail não migram facilmente para a Amazon WorkMail. Esses clientes exigem que o usuário execute etapas adicionais de configuração. Diferentes clientes de e-mail exigem a execução de ações diferentes.

- Microsoft Outlook no Windows – requer a reinicialização do Outlook. Na inicialização, é necessário escolher se você deseja continuar usando a caixa postal antiga ou usar uma caixa postal temporária. Escolha a opção de caixa de correio temporária. em seguida, reconfigure a caixa de correio do Microsoft Exchange.
- Microsoft Outlook no MacOS – quando o Outlook for reinicializado, você verá a seguinte mensagem: O Outlook foi redirecionado para o servidor ***orgname***.awsapps.com. Você quer que este servidor defina suas configurações? Aceite a sugestão.
- Correio no iOS – o aplicativo de e-mail não recebe mais e-mails e gera um erro Não é possível obter e-mails. Recrie e reconfigure a caixa de correio do Microsoft Exchange.

Desabilitar o modo de interoperabilidade e desativar o servidor de e-mail

Depois de configurar suas caixas de correio do Microsoft Exchange para a Amazon WorkMail, você pode desativar o modo de interoperabilidade. Se você não tiver migrado usuários ou registros, a desabilitação do modo de interoperabilidade não afetará suas configurações.

> **Warning**
>
> Antes de desabilitar o modo de interoperabilidade, conclua todas as etapas necessárias. Caso contrário, poderá resultar na devolução dos e-mails ou em comportamento indesejado. Caso a migração não tenha sido concluída, a desabilitação da interoperabilidade poderá causar interrupções na sua organização. Você não pode desfazer esta operação.

Para desabilitar o suporte ao modo de interoperabilidade

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, selecione Organizações e, em seguida, escolha a organização para a qual deseja desabilitar o modo de interoperabilidade.
3. Em Configurações da organização, escolha Desabilitar o modo de interoperabilidade.
4. Na caixa de diálogo Desabilitar o modo de interoperabilidade, insira o nome da organização e escolha Desabilitar o modo de interoperabilidade.

Depois de desativar o suporte à interoperabilidade, os usuários e grupos que não estão habilitados para a Amazon WorkMail são removidos do catálogo de endereços. Você ainda pode habilitar qualquer usuário ou grupo ausente usando o WorkMail console da Amazon, e eles serão adicionados ao catálogo de endereços. Os recursos do Microsoft Exchange não podem ser habilitados só serão exibidos no catálogo de endereços quando a etapa abaixo for concluída.

- Crie recursos na Amazon WorkMail — Você pode criar recursos na Amazon WorkMail e depois configurar delegados e opções de reserva para esses recursos. Para obter mais informações, consulte Trabalhar com recursos.
- Crie um registro AutoDiscover DNS — Configure um registro AutoDiscover DNS para todos os domínios de e-mail na organização. Isso permite que os usuários se conectem às suas WorkMail caixas de correio da Amazon a partir do Microsoft Outlook e de clientes móveis. Para obter mais informações, consulte Usar AutoDiscover para configurar endpoints.
- Mude seu registro MX DNS para a Amazon WorkMail — Para enviar todos os e-mails recebidos para a Amazon WorkMail, você deve trocar seu registro MX DNS para a Amazon. WorkMail As alterações dos registros DNS podem levar até 72 horas para serem propagadas para todos os servidores DNS.
- Desative seu servidor de e-mail — Depois de verificar se todos os e-mails estão sendo encaminhados diretamente para a Amazon WorkMail, você pode descomissionar seu servidor de e-mail se não pretender usá-lo daqui para frente.

Solução de problemas

As soluções para os erros mais comuns de WorkMail interoperabilidade e migração da Amazon estão listadas abaixo.

A URL do Exchange Web Services (EWS) é inválida ou inacessível – verifique se você tem a URL correta do EWS. Para ter mais informações, consulte Defina as configurações de disponibilidade na Amazon WorkMail.

Falha de conexão durante validação do EWS – este é um erro geral e pode ser causado por:

- Sem conexão à Internet no Microsoft Exchange.
- O firewall não está configurado para permitir o acesso da Internet. Verifique se a porta 443 (padrão das solicitações HTTPS) está aberta.

Se você confirmou a conexão à Internet e as configurações do firewall, mas o erro persistir, entre em contato com o AWS Support.

Nome de usuário e senha inválidos ao configurar a interoperabilidade do Microsoft Exchange – este é um erro geral e pode ser causado por:

- O nome de usuário não está no formato esperado. Use o seguinte padrão:

```
DOMAIN\username
```

- Seu servidor do Microsoft Exchange não está configurado para autenticação básica para o EWS. Para obter mais informações, consulte Virtual Directories: Exchange 2013 no blog do programa de recompensas do Microsoft MVP.

O usuário recebe e-mails com anexo winmail.dat — Isso pode acontecer quando um e-mail S/MIME criptografado é enviado do Exchange para a Amazon WorkMail e recebido no Outlook 2016 para Mac ou em um cliente IMAP. A solução é executar o seguinte comando no Shell de gerenciamento do Exchange.

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

Se você confirmou os pontos acima, mas o erro persistir, entre em contato com o AWS Support.

WorkMail Cotas da Amazon

A Amazon WorkMail pode ser usada tanto por clientes corporativos quanto por proprietários de pequenas empresas. Embora ofereçamos suporte à maioria dos casos de uso sem precisar alterar as cotas, também protegemos nossos usuários e a Internet contra o abuso do produto. Portanto,

alguns clientes podem encontrar cotas definidas por nós. Esta seção descreve essas cotas e como alterá-las.

Alguns valores de cota podem ser alterados e outros são cotas fixas que não podem ser alteradas. Para obter mais informações sobre como solicitar um aumento de cota, consulte Cotas de serviço da AWS no Referência geral da Amazon Web Services.

WorkMail Organização da Amazon e cotas de usuários

Você pode adicionar até 25 usuários à sua WorkMail organização Amazon para um teste gratuito de 30 dias. Após o término desse período, você será cobrado por todos os usuários ativos, a menos que você os remova ou feche sua WorkMail conta da Amazon.

Todas as mensagens enviadas para outro usuário são consideradas ao avaliar essas cotas. Elas incluem e-mails, solicitações de reunião, respostas de reuniões, solicitações de tarefas e mensagens encaminhadas ou redirecionadas automaticamente como resultado de uma regra.

> **Note**
>
> Ao fazer uma solicitação de aumento de cota somente para uma organização específica, inclua o nome da organização na solicitação.

Recurso	Cota padrão	Limite máximo de solicitações de alteração
WorkMail Organizações da Amazon por AWS conta	100	Podem ser aumentadas com base no tipo de diretório de uma organização. Você pode visualizar as cotas AWS Directory Service e solicitar aumentos no console AWS Directory Service. Para obter mais informações, consulte cotas de serviço no Referênci a geral da AWS.
Usuários por WorkMail organização da Amazon	1.000	Podem ser aumentados, dependendo do tipo de

Recurso	Cota padrão	Limite máximo de solicitações de alteração
		diretório da organização, como segue: • WorkMail Diretório Amazon: até 10 milhões de usuários • Simple AD ou AD Connector , grande: até 5.000 usuários* • Simple AD ou AD Connector , pequeno: até 500 usuários* • Microsoft AD, hospedado pelo AWS Directory Service: dependendo da configura ção, até 10 milhões de usuários, *Se você estiver usando o Simple AD ou o AD Connector , consulte AWS Directory Service para obter mais informações.
Usuários de avaliação gratuita	Até 25 usuários nos primeiros 30 dias	O período de avaliação gratuita só se aplica aos primeiros 25 usuários de uma organização. Os usuários adicionais não são incluídos na oferta de avaliação gratuita.

Recurso	Cota padrão	Limite máximo de solicitações de alteração
Destinatários por conta da AWS por dia	100.000 destinatários externos da organização, sem cota fixa de destinatários internos da organização	Não há limite máximo. No entanto, a Amazon WorkMail é um serviço de e-mail comercial e não deve ser usado para serviços de e-mail em massa. Para serviços de e-mail em massa, consulte Amazon SES ou Amazon Pinpoint.
Destinatários por conta da AWS por dia usando um dos domínios de teste	200 destinatários, independentemente do destino	O domínio de e-mail de teste não é destinado ao uso em longo prazo. Recomendamos adicionar seu próprio domínio e usá-lo como o domínio padrão.

As cotas de grupos são definidas pelo diretório subjacente.

WorkMail organização definindo cotas

Recurso	Cota padrão
Número de domínios por organização da Amazon WorkMail	1.000 Essa é uma cota fixa e não pode ser alterada.
Número de padrões do remetente em regras de fluxo de e-mail por regra	250 Essa é uma cota fixa e não pode ser alterada.
Número de padrões do remetente em regras de fluxo de e-mail por organização	1.000 Essa é uma cota fixa e não pode ser alterada.

Cotas por usuário

Todas as mensagens enviadas para outro usuário são consideradas ao avaliar essas cotas. Elas incluem e-mails, solicitações de reunião, respostas de reuniões, solicitações de tarefas e mensagens encaminhadas ou redirecionadas automaticamente como resultado de uma regra.

Recurso	Cota padrão	Cota máxima de solicitações de alteração
Tamanho máximo da caixa postal	50 GB Essa é uma cota fixa e não pode ser alterada.	Não aplicável
Número máximo de aliases por usuário	100 Essa é uma cota fixa e não pode ser alterada.	Não aplicável
Destinatários por usuário por dia usando seu domínio	10.000 destinatários externos da organização, sem cota fixa de destinatários internos da organização.	Não há limite máximo. No entanto, a Amazon WorkMail é um serviço de e-mail comercial e não deve ser usado para serviços de e-mail em massa. Para serviços de e-mail em massa, consulte Amazon SES ou Amazon Pinpoint.

Cotas de mensagens

Todas as mensagens enviadas para outro usuário são consideradas ao avaliar essas cotas. Elas incluem e-mails, solicitações de reunião, respostas de reuniões, solicitações de tarefas e mensagens encaminhadas ou redirecionadas automaticamente como resultado de uma regra.

Recurso	Cota padrão
Tamanho máximo de mensagens recebidas	29 MB de dados não codificados.

Recurso	Cota padrão
	As mensagens são recebidas em formato MIME. O tamanho máximo da mensagem MIME recebida é de 40 MB. Essa é uma cota fixa e não pode ser alterada.
Tamanho máximo de mensagens enviadas	29 MB de dados não codificados. As mensagens são enviadas em formato MIME. O tamanho máximo da mensagem MIME enviada é de 40 MB. Essa é uma cota fixa e não pode ser alterada.
Número máximo de destinatários por mensagem	500 Essa é uma cota fixa e não pode ser alterada.
Número máximo de anexos por mensagem	500 Essa é uma cota fixa e não pode ser alterada.

Trabalhar com organizações

Na Amazon WorkMail, sua organização representa os usuários da sua empresa. No WorkMail console da Amazon, você vê uma lista das organizações disponíveis. Se você não tiver nenhuma disponível, deverá criar uma organização para usar a Amazon WorkMail.

Tópicos

Criar uma organização

Para usar a Amazon WorkMail, você deve primeiro criar uma organização. Uma AWS conta pode ter várias WorkMail organizações da Amazon. Ao criar uma organização, você também seleciona um domínio para a organização e define configurações de diretório e criptografia do usuário.

Você pode criar um novo diretório de usuários ou integrar a Amazon WorkMail a um diretório existente. Você pode usar a Amazon WorkMail com um Microsoft Active Directory, AWS Managed Active Directory ou Simple AD local. Ao se integrar ao seu diretório local, você pode usar seus usuários e grupos existentes na Amazon WorkMail e os usuários podem entrar com suas credenciais existentes. Se você estiver usando um diretório on-premises, primeiro você deve definir um AD Connector no AWS Directory Service. O AD Connector sincroniza seus usuários e grupos com o catálogo de WorkMail endereços da Amazon e executa solicitações de autenticação de usuários. Para obter mais informações, consulte Active Directory Connector no Guia do administrador do AWS Directory Service.

Você também tem a opção de selecionar um AWS KMS key que a Amazon WorkMail usa para criptografar o conteúdo da caixa de correio. Você pode selecionar a chave mestra AWS gerenciada padrão para a Amazon WorkMail ou usar uma chave KMS existente em AWS Key Management Service (AWS KMS). Para obter informações sobre como criar chaves KMS, consulte Criar chaves

no Guia do desenvolvedor do AWS Key Management Service. Se você estiver conectado como usuário do AWS Identity and Access Management (IAM), torne-se administrador principal da chave KMS. Para obter mais informações, consulte Habilitar e desabilitar chaves no AWS Key Management ServiceGuia do desenvolvedor do .

Considerações

Lembre-se do seguinte ao criar uma WorkMail organização na Amazon:

- Atualmente, a Amazon WorkMail não oferece suporte aos serviços gerenciados do Microsoft Active Directory que você compartilha com várias contas.
- Se você tiver um Active Directory on-premises com Microsoft Exchange e AD Connector, recomendamos definir as configurações de interoperabilidade para sua organização. Isso permite que você minimize as interrupções para seus usuários ao migrar caixas de correio para a Amazon ou usar a Amazon WorkMail WorkMail para um subconjunto de suas caixas de correio corporativas. Para ter mais informações, consulte Interoperabilidade entre Amazon e WorkMail Microsoft Exchange.
- Se você selecionar a opção Domínio de teste gratuito, poderá começar a usar sua WorkMail organização Amazon com o domínio de teste fornecido. O domínio de teste usa o formato a seguir: *exemplo*.awsapps.com. Você pode usar o domínio de e-mail de teste com a Amazon WorkMail e outros AWS serviços compatíveis, desde que mantenha usuários habilitados em sua WorkMail organização Amazon. No entanto, não é possível usar o domínio de teste para outras finalidades. O domínio de teste pode ficar disponível para registro e uso por outros clientes se sua WorkMail organização Amazon não mantiver pelo menos um usuário habilitado.
- A Amazon WorkMail não oferece suporte a diretórios multirregionais.

Tópicos

Criar uma organização

Crie uma nova organização no WorkMail console da Amazon.

Para criar uma organização do

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. Na barra de navegação, selecione Organização.

   A página Organizações será exibida, mostrando suas organizações, se houver.
3. Escolha Criar organização.
4. Em Domínio de e-mail, selecione o domínio a ser usado para os endereços de e-mail da sua organização:

   - Domínio do Route 53 atual – Selecione um domínio atual que você gerencia com uma zona hospedada do Amazon Route 53 (Route 53).
   - Novo domínio do Route 53 — registre um novo nome de domínio do Route 53 para usar com a Amazon WorkMail.
   - Domínio externo – Insira um domínio atual que você gerencia com um provedor externo de Sistema de Nomes de Domínio (DNS).
   - Domínio de teste gratuito — Use um domínio de teste gratuito fornecido pela Amazon WorkMail. Você pode explorar a Amazon WorkMail usando um domínio de teste e depois adicionar um domínio à sua organização posteriormente.
5. (Opcional) Se seu domínio for gerenciado pelo Amazon Route 53, em zona hospedada do Route 53, selecione seu domínio do Route 53.
6. Em Alias, insira um alias exclusivo para sua organização.
7. Escolha Configurações avançadas e, em Diretório do usuário, selecione uma das seguintes opções:

   - Crie um novo WorkMail diretório da Amazon — Cria um novo diretório para adicionar e gerenciar seus usuários.
   - Usar diretório atual — Usa um diretório atual para gerenciar seus usuários, como Microsoft Active Directory, AWS Managed Active Directory ou Simple AD on-premises.
8. Em Criptografia, escolha uma das seguintes opções:

- Use uma chave WorkMail gerenciada pela Amazon — Cria uma nova chave de criptografia em sua conta.
- Usar chave KMS atual – Usa uma chave KMS atual que você já criou em AWS KMS.

9. Selecione Criar organização.

Se você usa um domínio externo, verifique o domínio adicionando os registros apropriados de texto (TXT) e troca de mensagens (MX) ao seu serviço de DNS. Os registros TXT permitem que você insira notas sobre o serviço de DNS. Os registros MX especificam o servidor de e-mail de entrada.

Certifique-se de definir seu domínio como padrão para sua organização. Para obter mais informações, consulte Escolher o domínio padrão e Verificar domínios.

Quando sua organização está Ativa, você pode adicionar usuários a ela e configurar seus clientes de e-mail. Para obter mais informações, consulte Incluir um usuário Configurar clientes de e-mail para a Amazon WorkMail.

Visualizar de detalhes da organização

Cada uma de suas WorkMail organizações da Amazon pode exibir uma página de detalhes da organização. A página mostra informações sobre a organização, incluindo IDs que você pode usar com a AWS Command Line Interface. As mensagens na página também podem mostrar todas as etapas necessárias para concluir a configuração e a organização, como um domínio não verificado ou a falta de usuários. As mensagens também fornecem a primeira etapa para configurar um determinado cliente de e-mail.

Para visualizar detalhes de uma organização

1. Na barra de navegação, selecione Organização.

   A página Organizações será exibida, mostrando suas organizações.

2. Escolha a organização que deseja visualizar.

Integrando uma Amazon WorkDocs ou WorkSpaces um diretório

Para usar a Amazon WorkMail com a Amazon WorkDocs ou WorkSpaces, crie um diretório compatível usando as etapas a seguir.

Para adicionar uma Amazon WorkDocs ou um WorkSpaces diretório compatível

1. Crie um diretório compatível usando Amazon WorkDocs ou WorkSpaces.

   a. Para obter WorkDocs instruções sobre a Amazon, consulte Introdução ao Quick Start no Guia de WorkDocs Administração da Amazon.

   b. Para obter WorkSpaces instruções, consulte Comece a usar o Amazon WorkSpaces Quick Setup no Guia de WorkSpaces Administração da Amazon.

2. No WorkMail console da Amazon, crie sua WorkMail organização Amazon e escolha usar seu diretório existente para ela. Para ter mais informações, consulte Criar uma organização.

Estados e descrições da organização

Depois de criar uma organização, ela pode ter um dos estados a seguir.

Estado	Descrição
Ativo	Sua organização é íntegra e está pronta para uso.
Criando	Um fluxo de trabalho está trabalhando para criar sua organização.
Com falha	Não foi possível criar sua organização.
Impaired (Degradado)	Foi detectado um problema ou uma falha na sua organização.
Inativo	Sua organização está inativa.
Requested (Solicitado)	Sua solicitação de criação de organização está na fila, aguardando a criação.
Validating	A integridade de todas as configurações da organização está sendo verificada.

Excluir uma organização

Se você não quiser mais usar a Amazon WorkMail para o e-mail da sua organização, você pode excluir sua organização da Amazon WorkMail.

> **Note**
>
> Essa operação não pode ser desfeita. Não será possível recuperar os dados da caixa de correio após a exclusão de uma organização.

Como excluir uma organização

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. Na tela Organizações, na lista de organizações, selecione a organização a ser excluída e escolha Excluir.
3. Em Excluir organização, escolha se deseja excluir ou manter o diretório de usuário atual e, em seguida, insira o nome da organização.
4. Escolha Excluir organização.

> **Note**
>
> Se você não forneceu seu próprio diretório para a Amazon WorkMail, criaremos um para você. Se você mantiver esse diretório existente ao excluir a organização, você será cobrado por ele, a menos que esteja sendo usado pela Amazon WorkMail WorkDocs, Amazon ou WorkSpaces. Para obter informações sobre definição de preços, consulte Outra definição de preço de tipos de diretórios.
> Para excluir o diretório, ele não pode ter outras aplicações da AWS habilitadas. Para obter mais informações, consulte Excluir um diretório do Simple AD ou Excluir um diretório do AD Connector no Guida do administrador do AWS Directory Service.

Você pode receber uma mensagem de erro inválida do conjunto de regras do Amazon Simple Email Service (Amazon SES) ao tentar excluir uma organização. Se você receber esse erro, edite a regra do Amazon SES no console do Amazon SES e remova o conjunto de regras inválido. A regra que você edita deve ter seu ID de WorkMail organização da Amazon no nome da regra. Para obter mais informações sobre a edição das regras do Amazon SES, consulte Criação de regras de recebimento no Guia do desenvolvedor do Amazon Simple Email Service.

Se você precisar descobrir qual conjunto de regras é inválido, salve a regra primeiro. Uma mensagem de erro será exibida para o conjunto de regras.

Encontrando um endereço de e-mail

Você pode descobrir se um endereço de e-mail é usado em sua organização por usuário, recurso ou grupo.

Para encontrar um endereço de e-mail

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome de uma organização.
3. Na página Organização, escolha Localizar endereço de e-mail.
4. Selecione a opção Pesquisar.

Trabalhar com configurações da organização

As seções a seguir explicam como usar as configurações disponíveis para WorkMail organizações da Amazon. As configurações que você escolher serão aplicadas a toda a organização.

Tópicos

- Habilitar a migração de caixa de correio
- Habilitar o registro no diário
- Habilitar a interoperabilidade

- Habilitar gateways SMTP
- Gerenciar fluxos de e-mail
- Aplicar políticas DMARC em e-mails recebidos

Habilitar a migração de caixa de correio

Você habilita a migração de caixas de correio quando deseja transferir caixas de correio de uma fonte, como Microsoft Exchange ou G Suite Basic, para a Amazon. WorkMail Você habilita a migração como parte de um processo de migração maior. Para obter mais informações, incluindo o passo a passo, consulte Migração para a Amazon WorkMail na seção Conceitos básicos deste guia.

Habilitar o registro no diário

É possível habilitar o registro no diário para registrar comunicações de e-mail. Ao usar o registro no diário, você normalmente usa ferramentas integradas de arquivamento e eDiscovery de terceiros. Isso garante que as regulamentações de conformidade de armazenamento de e-mails para proteção de privacidade, armazenamento de dados e proteção de informações sejam atendidas.

Para obter mais informações, incluindo o passo a passo, consulte Usando o registro no diário de e-mail com o Amazon WorkMail na seção Conceitos básicos deste guia.

Habilitar a interoperabilidade

A interoperabilidade permite que você migre do Microsoft Exchange e use a Amazon WorkMail como um subconjunto de suas caixas de correio corporativas. Para obter mais informações, incluindo o passo a passo, consulte Defina as configurações de disponibilidade na Amazon WorkMail na seção Conceitos básicos deste guia.

Habilitar gateways SMTP

Você habilita gateways do Simple Mail Transfer Protocol (SMTP) para usar com regras de fluxo de e-mails enviados. As regras de fluxo de e-mail de saída permitem que você encaminhe mensagens de e-mail enviadas da sua WorkMail organização Amazon por meio de um gateway SMTP. Para ter mais informações, consulte Ações de regras para e-mails enviados.

> **Note**
>
> Os gateways SMTP configurados para regras de fluxo de e-mails enviados devem ser compatíveis com o Transport Layer Security (TLS) v1.2 usando certificados das principais autoridades de certificação. Somente a autenticação básica é compatível.

Para configurar um gateway SMTP

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome de uma organização.
3. No painel de navegação, selecione Organization settings (Configurações da organização).

   A página de Configurações da organização será exibida, mostrando um conjunto de guias.
4. Escolha a guia Gateways SMTP e, em seguida, escolha Criar gateway.
5. Insira o seguinte:

   - Nome do gateway – Insira um nome exclusivo.
   - Endereço do gateway – Insira o nome do host ou endereço IP do gateway.
   - Número da porta – Insira o número da porta do gateway.
   - Nome de usuário – Insira um nome de usuário.
   - Senha – Insira uma senha forte.
6. Escolha Criar.

   O gateway SMTP estará disponível para uso com regras de fluxo de e-mails enviados.

Quando você configura um gateway SMTP para usar com uma regra de fluxo de e-mails enviados, as mensagens enviadas tentam combinar a regra com um gateway SMTP. As mensagens que correspondem à regra são roteadas para o gateway SMTP correspondente, que passa a processar o restante da entrega do e-mail.

Se WorkMail a Amazon não conseguir acessar o gateway SMTP, o sistema devolverá a mensagem de e-mail ao remetente. Se isso ocorrer, siga as etapas anteriores para corrigir as configurações do gateway.

Gerenciar fluxos de e-mail

Para ajudar a gerenciar e-mails, você pode configurar regras de fluxo de e-mails. As regras de fluxo de e-mail podem realizar uma ou mais ações em mensagens de e-mail com base em seus endereços ou domínios. Você pode usar as regras de fluxo de e-mails em endereços de e-mail ou domínios do "remetente" e do "destinatário".

Para criar uma regra de fluxo de e-mail, especifique uma ação da regra que se aplica a um e-mail quando houver correspondência com um padrão de regra específico.

Tópicos

Ações de regras para e-mails recebidos

As regras de fluxo de e-mails recebidos ajudam a evitar que mensagens indesejadas cheguem às caixas de correio dos usuários. As regras de fluxo de entrada de e-mails, também chamadas de ações de regras, se aplicam automaticamente a todas as mensagens de e-mail enviadas a qualquer pessoa dentro da sua WorkMail organização Amazon. Isso difere das regras de e-mail para caixas de correio individuais.

> **Note**
>
> Essas regras podem ser usadas com uma função do AWS Lambda para processar e-mails recebidos antes que sejam entregues nas caixas de correio dos usuários. Para obter mais

informações sobre o uso do Lambda com a Amazon WorkMail, consulte. Configurando AWS Lambda para a Amazon WorkMail Para obter mais informações sobre o Lambda, consulte o Manual do desenvolvedor do AWS Lambda.

As regras de fluxo de entrada de e-mails, também chamadas de ações de regras, se aplicam automaticamente a todas as mensagens de e-mail enviadas a qualquer pessoa dentro da WorkMail organização Amazon. Isso difere das regras de e-mail para caixas de correio individuais.

As ações de regra a seguir definem a forma de lidar com e-mails recebidos. Para cada regra, especifique padrões de remetentes e destinatários e uma das ações a seguir.

Ação	Descrição
Eliminar e-mail	A mensagem de e-mail é ignorada. Ele não é entregue, e o remetente não é notificado sobre isso.
Enviar resposta de devolução	A mensagem de e-mail não é entregue, e o remetente é notificado sobre isso por uma mensagem de devolução.
Deliver to junk folder	A mensagem de e-mail é entregue às pastas de spam ou lixo eletrônico dos usuários, mesmo que não tenha sido originalmente identificada como spam pelo sistema de detecção de WorkMail spam da Amazon.
Padrão	A mensagem de e-mail é entregue após ser verificada pelo sistema de detecção WorkMail de spam da Amazon. O spam é enviado para a lixeira. Todos as outras mensagens de e-mail são entregues na caixa de entrada. Outras regras de fluxo de e-mail com um padrão de remetente menos específico são ignoradas. Para adicionar exceções ao domínio com base nas regras de fluxo de e-mail,

Ação	Descrição
	configure a ação padrão com mais de um padrão específico de remetente. Para ter mais informações, consulte Padrões de remetente e destinatário.
Never deliver to junk folder	A mensagem de e-mail é sempre entregue nas caixas de entrada dos usuários, mesmo que seja identificada como spam pelo sistema de detecção de WorkMail spam da Amazon. **Important** Não utilizar o sistema padrão de detecção de spam pode expor seus usuários a conteúdo de alto risco dos endereços especificados por você.
Executar AWS Lambda	Transmite a mensagem de e-mail para uma função do Lambda para processamento antes ou durante a entrega nas caixas de entrada dos usuários.

Note

O e-mail de entrada é entregue primeiro para o Amazon SES e depois para a Amazon WorkMail. Se o Amazon SES bloquear um e-mail recebido, as ações de regra não serão aplicadas. Por exemplo, o Amazon SES bloqueia uma mensagem de e-mail quando um vírus conhecido é detectado ou devido a regras explícitas de filtragem de IP. Nada acontecerá se você especificar uma ação de regra, como Default (Padrão), Deliver to junk folder (Enviar para a lixeira) ou Never deliver to junk folder (Nunca enviar para a lixeira).

Ações de regras para e-mails enviados

As regras de fluxo de e-mails enviados podem ser usadas para direcionar mensagens de e-mail via gateways SMTP ou para impedir que os remetentes enviem e-mails a destinatários específicos. Para obter mais informações sobre gateways SMTP, consulte Habilitar gateways SMTP.

As regras de fluxo de e-mails enviados também podem ser usadas para passar a mensagem de e-mail por uma função do AWS Lambda para processamento após o envio. Para obter mais informações sobre o Lambda, consulte o Manual do desenvolvedor do AWS Lambda.

As ações de regra a seguir definem a forma de lidar com e-mails enviados. Para cada regra, especifique padrões de remetentes e destinatários e uma das ações a seguir.

Ação	Descrição
Padrão	A mensagem de e-mail é enviada por meio do fluxo normal.
Eliminar e-mail	A mensagem de e-mail é descartada. Ele não é enviado, e o remetente não é notificado.
Enviar resposta de devolução	A mensagem de e-mail não é enviada, e o remetente recebe uma notificação dizendo que o administrador bloqueou a mensagem de e-mail.
Rotear para gateway SMTP	A mensagem de e-mail é enviada por meio de um gateway SMTP configurado.
Executar o Lambda	Transmite a mensagem de e-mail para uma função do Lambda para processamento antes ou dutante o envio da mensagem de e-mail.

Padrões de remetente e destinatário

Uma regra de fluxo de e-mail pode ser aplicada a um endereço de e-mail específico ou a todos os endereços de e-mail de um domínio ou conjunto de domínios. Você define um padrão para determinar os endereços de e-mail aos quais a regra se aplica.

Ambos os padrões de remetente e destinatário tomam uma das seguintes formas:

- Um endereço de e-mail corresponde a um único endereço de e-mail, por exemplo:

```
mailbox@example.com
```

- Um nome de domínio corresponde a todos os endereços de e-mail desse domínio, por exemplo:

```
example.com
```

- Um domínio curinga corresponde a todos os endereços de e-mail desse domínio e a todos os subdomínios dele. Um curinga aparece somente na frente do domínio. Por exemplo:

```
*.example.com
```

- A estrela corresponde a qualquer endereço de e-mail de qualquer domínio.

```
*
```

> **Note**
>
> O símbolo + não é válido dentro dos padrões de remetente ou de destinatário.

Vários padrões podem ser especificados para uma regra. Para obter mais informações, consulte Ações de regras para e-mails enviados e Ações de regras para e-mails recebidos.

As regras de fluxo de e-mails recebidos são aplicadas se o cabeçalho `Sender` ou `From` em uma mensagem recebida corresponder a algum dos padrões. Se houver, o endereço `Sender` é correspondido primeiro. O endereço `From` é correspondido se não houver o cabeçalho `Sender` ou se o cabeçalho `Sender` não for correspondente a nenhuma regra. Se vários destinatários da mensagem de e-mail corresponderem a diferentes regras, cada regra será aplicada aos destinatários correspondentes.

As regras de fluxo de e-mails enviados são aplicadas se o destinatário e o cabeçalho `Sender` ou `From` em uma mensagem enviada corresponder a algum dos padrões. Se vários destinatários da mensagem de e-mail corresponderem a diferentes regras, cada regra será aplicada aos destinatários correspondentes.

Se várias regras corresponderem, a ação da regra mais específica será aplicada. Por exemplo, uma regra de um endereço de e-mail específico tem precedência sobre uma regra para todo o domínio. Se várias regras tiverem o mesmo grau de especificidade, a ação mais restritiva será aplicada. Por exemplo, a ação Drop (Descartar) tem precedência sobre a ação Bounce (Devolver). A ordem de precedência para as ações é a mesma ordem em que aparecem listadas em Ações de regras para e-mails recebidos e Ações de regras para e-mails enviados.

> **Note**
>
> Tenha cuidado ao criar regras com padrões de remetente sobrepostos com a ação Drop ou Bounce. Uma ordem de precedência inesperada pode resultar em muitas mensagens de e-mail recebidas não entregues.

Criar uma regra de fluxo de e-mail

As regras de fluxo de e-mail aplicam ações de regra às mensagens de e-mail recebidas e enviadas. As ações se aplicam quando as mensagens correspondem a um padrão específico. As novas regras de fluxo de e-mail entram em vigor imediatamente.

Para criar uma regra de fluxo de e-mail

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome de uma organização.
3. No painel de navegação, selecione Organization settings (Configurações da organização).

   A página de Configurações da organização será exibida, mostrando um conjunto de guias. Nessa página, você pode criar regras de entrada ou saída. Os tópicos a seguir explicam como criar os dois tipos de regras.

   Para criar regras de entrada

   1. Escolha a guia Regras de entrada e, em seguida, escolha Editar regra.
   2. Na caixa Nome da regra, insira um nome exclusivo.

3. Em Ação, abra a lista e selecione uma ação. Cada item da lista contém uma descrição, e alguns fornecem links Saiba mais.

> **Note**
>
> Se você escolher a ação Executar o Lambda, controles adicionais aparecerão: Para obter informações sobre como usar esses controles, consulte a próxima seção, Configurando AWS Lambda para a Amazon WorkMail.

4. Em Domínios ou endereços do remetente, insira os domínios ou endereços do remetente que você deseja que a regra se aplique.
5. Em Domínios ou endereços de destino, insira qualquer combinação de domínios de destino e endereços de e-mail.
6. Escolha Criar.

Para criar regras de saída

1. Escolha a guia Regras de saída e, em seguida, escolha Criar.
2. Na caixa Nome da regra, insira um nome exclusivo.
3. Em Ação, abra a lista e selecione uma ação. Cada item da lista contém uma descrição, e alguns fornecem links Saiba mais.

> **Note**
>
> Se você escolher a ação Executar o Lambda, controles adicionais aparecerão. Para obter mais informações sobre o uso desses controles, consulte a próxima sessão,Configurando AWS Lambda para a Amazon WorkMail.

4. Em Domínios ou endereços do remetente, insira qualquer combinação de domínios de remetente e endereços de e-mail válidos.
5. Em Domínios ou endereços de destino, insira qualquer combinação de domínios de destino e endereços de e-mail válidos.
6. Escolha Criar.

É possível testar a regra de fluxo de e-mail recém-criada. Para ter mais informações, consulte Testar uma regra de fluxo de e-mail.

Editar regras de fluxo de e-mail

Você edita as regras de fluxo de e-mail sempre que precisar alterar uma ou mais ações de regra para mensagens de e-mail. As etapas desta seção se aplicam às mensagens de e-mail recebidas e enviadas.

Para editar regras de fluxo de e-mail

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome de uma organização.
3. No painel de navegação, selecione Organization settings (Configurações da organização).

   A página de Configurações da organização será exibida, mostrando um conjunto de guias.
4. Escolha as guias Regras de entrada ou Regras de saída.
5. Escolha o botão de opção próximo à regra a ser alterada e selecione Editar.
6. Altere a ação ou ações na regra conforme necessário e escolha Salvar.

Configurando AWS Lambda para a Amazon WorkMail

Use a ação Executar o Lambda em regras de fluxo de e-mails de entrada e saída para transmitir as mensagens de e-mail que correspondem às regras para uma função do AWS Lambda para processamento.

Escolha entre as seguintes configurações para uma ação Run Lambda na Amazon. WorkMail

Configuração síncrona de Executar o

> As mensagens de e-mail que correspondem à regra de fluxo são transmitidas para uma função do Lambda para processamento antes de serem enviadas ou entregues. Use essa configuração para modificar o conteúdo do e-mail. Você também pode controlar o fluxo de e-mails de entrada ou saída para diferentes casos de uso. Por exemplo, uma regra transmitida para uma função do Lambda pode bloquear a entrega de mensagens de e-mail confidenciais, remover anexos ou adicionar avisos de isenção de responsabilidade.

Configuração assíncrona de Executar o Lambda

As mensagens de e-mail que correspondem à regra de fluxo são transmitidas para uma função do Lambda para processamento enquanto são enviadas ou entregues. Essa configuração não afeta a entrega de e-mail e é usada para tarefas como coletar métricas para mensagens de e-mail de entrada ou saída.

Independentemente de você escolher uma configuração síncrona ou assíncrona, o objeto de evento transmitido para a função do Lambda contém metadados para o evento de e-mail de entrada ou saída. Também é possível usar o ID da mensagem nos metadados para acessar o conteúdo completo da mensagem de e-mail. Para ter mais informações, consulte Recuperar conteúdo de mensagens com o AWS Lambda. Para obter mais informações sobre eventos de e-mail, consulte Dados de eventos do Lambda.

Para obter mais informações sobre as regras de fluxo de e-mails enviados e recebidos, consulte Gerenciar fluxos de e-mail. Para obter mais informações sobre o Lambda, consulte o Manual do desenvolvedor do AWS Lambda.

> **Note**
>
> Atualmente, as regras de fluxo de e-mail do Lambda fazem referência somente às funções do Lambda na mesma região da AWS e da organização Conta da AWS da Amazon WorkMail que está sendo configurada.

Começando a usar AWS Lambda para a Amazon WorkMail

Para começar a usar AWS Lambda com a Amazon WorkMail, recomendamos implantar a função WorkMail Hello World Lambda AWS Serverless Application Repository na sua conta. A função tem todos os recursos necessários e as permissões configuradas para você. Para obter mais exemplos, consulte o amazon-workmail-lambda-templatesrepositório em. GitHub

Se você escolher criar sua própria função do Lambda, deverá configurar as permissões usando a AWS Command Line Interface (AWS CLI). Para usar o seguinte comando de exemplo, faça como a seguir:

- Substitua `MY_FUNCTION_NAME` pelo nome da sua função do Lambda.

- `REGION`Substitua pela sua região WorkMail da Amazon AWS. As WorkMail regiões disponíveis da Amazon incluem `us-east-1` (Leste dos EUA (Norte da Virgínia)), `us-west-2` (Oeste dos EUA (Oregon)) e `eu-west-1` (Europa (Irlanda)).
- Substitua `AWS_ACCOUNT_ID` pelo seu ID de Conta da AWS de 12 dígitos.
- `WORKMAIL_ORGANIZATION_ID`Substitua pelo ID da sua WorkMail organização na Amazon. Você pode encontrá-lo no cartão da sua organização na página Organizações.

```
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 obter mais informações sobre como usar o AWS CLI, consulte o Manual do usuário do AWS Command Line Interface.

Configurar regras síncronas de Executar o Lambda

Para configurar uma regra síncrona de Executar o Lambda, crie uma regra de fluxo de e-mail com a ação Executar o Lambda e marque a caixa de seleção Executar de forma síncrona. Para obter mais informações sobre como criar regras de fluxo de e-mail, consulte Criar uma regra de fluxo de e-mail.

Para concluir a criação da regra síncrona, adicione o nome do recurso da Amazon (ARN) do Lambda e configure as opções a seguir.

Ação de fallback

A ação que a Amazon WorkMail aplica se a função Lambda não for executada. Essa ação também se aplicará a todos os destinatários omitidos da resposta do Lambda se o sinalizador allRecipients não for definido. A Ação de fallback não pode ser outra ação do Lambda.

Tempo limite da regra (em minutos)

O período durante o qual a função Lambda é repetida se a Amazon WorkMail não a invocar. A Ação de fallback é aplicada no final desse período.

> **Note**
>
> Regras síncronas de Executar o Lambda oferecem suporte apenas à condição de destino *****.

Dados de eventos do Lambda

A função do Lambda é acionada usando os seguintes dados de evento. A apresentação dos dados varia dependendo da linguagem de programação usada para a função do 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
}
```

O JSON do evento inclui os seguintes dados:

summaryVersion

O número da versão para `LambdaEventData`. Isso só é atualizado quando você faz uma alteração incompatível com versões anteriores. `LambdaEventData`

envelope

O envelope da mensagem de e-mail, que inclui os campos a seguir:

mailFrom

O endereço De, que normalmente corresponde ao endereço de e-mail do usuário que enviou a mensagem. Se o usuário enviou a mensagem como outro usuário ou em nome de outro usuário, o campo mailFrom retornará o endereço de e-mail do usuário em cujo nome a mensagem foi enviada, e não o endereço do remetente real.

recipients

Uma lista de endereços de e-mail dos destinatários. A Amazon WorkMail não faz distinção entre To, CC ou BCC.

> **Note**
>
> Para regras de fluxo de e-mail de entrada, essa lista inclui destinatários em todos os domínios da WorkMail organização da Amazon na qual você criou a regra. A função do Lambda é invocada separadamente para cada conversão de SMTP do remetente, e o campo dos destinatários listará os destinatários dessa conversão de SMTP. Destinatários com domínios externos não são incluídos.

sender (remetente)

O endereço de e-mail do usuário que enviou a mensagem de e-mail em nome de outro usuário. Esse campo é definido somente quando uma mensagem de e-mail é enviada em nome de outro usuário.

subject

A linha de assunto do e-mail. Truncado quando exceder o limite de 256 caracteres.

messageId

Um ID exclusivo usado para acessar o conteúdo completo da mensagem de e-mail ao usar o SDK do Amazon WorkMail Message Flow.

invocationId

O ID de uma invocação exclusiva do Lambda. Esse ID permanece o mesmo quando uma função Lambda é chamada mais de uma vez para a mesma. LambdaEventData Use para detectar novas tentativas e evitar duplicações.

flowDirection

Indica a direção do fluxo de e-mail, ENTRADA ou SAÍDA.

truncado

Aplicável ao tamanho da carga útil, não ao tamanho da linha de assunto. Quando `true`, o tamanho da carga ultrapassa o limite de 128 KB. Portanto, a lista de destinatários é truncada para ater-se ao limite.

Esquema de resposta síncrona de Executar o Lambda

Quando uma regra de fluxo de e-mail com uma ação síncrona Executar Lambda corresponde a uma mensagem de e-mail de entrada ou saída, a Amazon WorkMail chama a função Lambda configurada e espera pela resposta antes de agir na mensagem de e-mail. A função do Lambda retorna uma resposta de acordo com um esquema predefinido que lista as ações, os tipos de ação, os parâmetros aplicáveis e os destinatários aos quais se aplica a ação.

O esquema a seguir é um exemplo de resposta síncrona de Executar o Lambda . As respostas variam de acordo com a linguagem de programação usada para a função do Lambda.

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

A resposta JSON inclui os dados a seguir.

ação

A ação a ser executada para os destinatários.

type

O tipo de ação. Os tipos de ação não são retornados para ações assíncronas de Executar o Lambda.

Os tipos de ação de regra de entrada incluem BOUNCE, DROP, DEFAULT, BYPASS_SPAM_CHECK e MOVE_TO_JUNK. Para ter mais informações, consulte Ações de regras para e-mails recebidos.

Os tipos de ação de regra de saída incluem BOUNCE, DROP e DEFAULT. Para ter mais informações, consulte Ações de regras para e-mails enviados.

parâmetros

Parâmetros de ação adicionais. Compatível com o tipo de ação BOUNCE como um objeto JSON com a chave bounceMessage e o valor string. Essa mensagem de devolução é usada para criar a mensagem de e-mail de devolução.

recipients

Lista de endereços de e-mail nos quais a ação deve ser executada. É possível adicionar novos destinatários à resposta mesmo que eles não tenham sido incluídos na lista de destinatários original. Esse campo não será obrigatório se allRecipients for verdadeiro para uma ação.

> **Note**
>
> Quando uma ação do Lambda é chamada para e-mail de entrada, só é possível adicionar novos destinatários da sua organização. Os novos destinatários são adicionados à resposta como BCC.

allRecipients

Quando verdadeiro, aplica a ação a todos os destinatários que não estão sujeitos a outra ação específica na resposta do Lambda.

Limites da ação síncrona de Executar o Lambda

Os seguintes limites se aplicam quando a Amazon WorkMail invoca funções do Lambda para ações síncronas do Run Lambda:

- As funções do Lambda devem responder em até 15 segundos ou ser tratadas como invocações com falha.

> **Note**
>
> O sistema repete a invocação para o intervalo de Tempo limite da regra especificado por você.

- Respostas da função do Lambda de até 256 KB são permitidas.
- Até 10 ações exclusivas são permitidas na resposta. As ações maiores que 10 estão sujeitas à Ação de fallbackconfigurada.
- Até 500 destinatários são permitidos para funções do Lambda de saída.
- O valor máximo de Tempo limite da regra é 240 minutos. Se o valor mínimo de 0 estiver configurado, não haverá novas tentativas antes que a Amazon WorkMail aplique a ação de fallback.

Falhas na ação síncrona de Executar o Lambda

Se a Amazon não WorkMail conseguir invocar sua função do Lambda devido a um erro, resposta inválida ou tempo limite do Lambda, a WorkMail Amazon tentará novamente a invocação com um atraso exponencial que diminui a taxa de processamento até que o período de tempo limite da regra seja concluído. Depois, a Ação de fallback é aplicada a todos os destinatários da mensagem de e-mail. Para ter mais informações, consulte Configurar regras síncronas de Executar o Lambda .

Exemplos de resposta síncrona de Executar o Lambda

Os exemplos a seguir demonstram a estrutura de respostas síncronas comuns de Executar o Lambda.

Example : Remover destinatários especificados de uma mensagem de e-mail

O exemplo a seguir demonstra a estrutura de uma resposta síncrona de Executar o Lambda para remover destinatários de uma mensagem de e-mail.

```
{
    "actions": [
      {
        "action": {
```

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

Example : Devolver com uma mensagem de e-mail personalizada

O exemplo a seguir demonstra a estrutura de uma resposta síncrona de Executar o Lambda para devolução de uma mensagem de e-mail personalizada.

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

Example : Adicionar destinatários a uma mensagem de e-mail

O exemplo a seguir demonstra a estrutura de uma resposta síncrona de Executar o Lambda para adicionar destinatários à mensagem de e-mail. Isso não atualiza os campos Para nem CC da mensagem de e-mail.

```
{
    "actions": [
```

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

Para obter mais exemplos de código para usar ao criar funções do Lambda para ações do Run Lambda, consulte os modelos do Amazon Lambda. WorkMail

Mais informações sobre o uso do Lambda com a Amazon WorkMail

Também é possível acessar o conteúdo completo da mensagem de e-mail que aciona a função do Lambda. Para ter mais informações, consulte Recuperar conteúdo de mensagens com o AWS Lambda.

Recuperar conteúdo de mensagens com o AWS Lambda

Depois de configurar uma AWS Lambda função para gerenciar fluxos de e-mail para a Amazon WorkMail, você pode acessar o conteúdo completo das mensagens de e-mail que são processadas usando o Lambda. Para obter mais informações sobre como começar a usar o Lambda for Amazon WorkMail, consulte. Configurando AWS Lambda para a Amazon WorkMail

Para acessar o conteúdo completo das mensagens de e-mail, use a `GetRawMessageContent` ação na API Amazon WorkMail Message Flow. O ID da mensagem de e-mail que é transmitido para sua função do Lambda na invocação envia uma solicitação para a API. Em seguida, a API responde com o conteúdo MIME completo da mensagem de e-mail. Para obter mais informações, consulte Amazon WorkMail Message Flow na Amazon WorkMail API Reference.

O exemplo a seguir mostra como uma função do Lambda usando o ambiente de runtime do Python pode recuperar o conteúdo completo da mensagem.

> **Tip**
>
> Se você começar implantando a função Amazon WorkMail Hello World Lambda na sua conta, AWS Serverless Application Repository o sistema criará uma função Lambda na sua conta com todos os recursos e permissões necessários. Você pode, então, adicionar sua lógica de negócios à função do Lambda com base no seu 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 obter exemplos mais detalhados de formas de analisar o conteúdo das mensagens que estão em trânsito, consulte o amazon-workmail-lambda-templatesrepositório em GitHub.

> **Note**
>
> Você só usa a API Amazon WorkMail Message Flow para acessar mensagens de e-mail em trânsito. As mensagens só podem ser acessadas em até 24 horas após serem enviadas ou recebidas. Para acessar mensagens programaticamente na caixa de correio de um usuário, use um dos outros protocolos suportados pela Amazon WorkMail, como IMAP ou Exchange Web Services (EWS).

Atualização do conteúdo de mensagens com o AWS Lambda

Depois de configurar uma AWS Lambda função síncrona para gerenciar fluxos de e-mail, você pode usar a `PutRawMessageContent` ação na API de fluxo de WorkMail mensagens da Amazon para atualizar o conteúdo das mensagens de e-mail em trânsito. Para obter mais informações sobre como começar a usar as funções Lambda para a Amazon WorkMail, consulte. Configurar

regras síncronas de Executar o Lambda Para obter mais informações sobre a API, consulte PutRawMessageContent.

> **Note**
>
> A PutRawMessageContent API requer o boto3 1.17.8, ou você pode adicionar uma camada à sua função Lambda. Para baixar a versão correta do boto3, consulte a página de inicialização em. GitHub Para obter mais informações sobre como adicionar camadas, consulte Configurar uma função para usar camadas.
> Confira a seguir um exemplo de camada: `"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`. Neste exemplo, substitua `${AWS::Region}` por uma região da AWS apropriada, como us-east-1.

> **Tip**
>
> Se você começar implantando a função Amazon WorkMail Hello World Lambda do AWS Serverless Application Repository em sua conta, o sistema criará uma função Lambda em sua conta com os recursos e permissões necessários. Você pode, então, adicionar sua lógica de negócios à função do Lambda com base no seu caso de uso.

À medida que avança, lembre-se do seguinte:

- Use a GetRawMessageContentAPI para recuperar o conteúdo original da mensagem. Para obter mais informações, consulte Recuperar conteúdo de mensagens com o AWS Lambda.
- Depois de ter a mensagem original, altere o conteúdo MIME. Ao terminar, atualize a mensagem para um bucket do Amazon Simple Storage Service (Amazon S3) na sua conta. Certifique-se de que o bucket do S3 use o mesmo que suas Conta da AWS WorkMail operações da Amazon e que use a mesma região da AWS que suas chamadas de API.
- Para WorkMail que a Amazon processe solicitações, seu bucket do S3 deve ter a política correta para acessar o objeto do S3. Para ter mais informações, consulte Example S3 policy.
- Use a PutRawMessageContentAPI para enviar o conteúdo atualizado da mensagem de volta para a Amazon WorkMail.

> **Note**
>
> A `PutRawMessageContent` API garante que o conteúdo MIME da mensagem atualizada atenda aos padrões RFC, bem como aos critérios mencionados no tipo de RawMessageContentdados. Os e-mails recebidos em sua WorkMail organização Amazon nem sempre atendem a esses padrões, então a `PutRawMessageContent` API pode rejeitá-los. Nesses casos, você pode consultar a mensagem de erro retornada para obter mais informações sobre como corrigir qualquer problema.

Example Exemplo de política do 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/*"
                }
            }
        }
    ]
}
```

O exemplo a seguir mostra como uma função do Lambda usa o runtime do Python para atualizar o assunto de uma mensagem de e-mail em trânsito.

```
    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="Your-S3-Bucket", Key=key)

        # Update the email in WorkMail
        s3_reference = {
            'bucket': "Your-S3-Bucket",
            'key': key
        }
        content = {
            's3Reference': s3_reference
        }
        workmail.put_raw_message_content(messageId=msg_id, content=content)
```

Para obter mais exemplos de maneiras de analisar o conteúdo de mensagens em trânsito, consulte o amazon-workmail-lambda-templatesrepositório em. GitHub

Gerenciando o acesso à API Amazon WorkMail Message Flow

Use políticas AWS Identity and Access Management (IAM) para gerenciar o acesso à API Amazon WorkMail Message Flow.

A API Amazon WorkMail Message Flow funciona com um único tipo de recurso, uma mensagem de e-mail em trânsito. Cada mensagem de e-mail em trânsito tem um nome de recurso da Amazon (ARN) exclusivo associado a ela.

O exemplo a seguir mostra a sintaxe de um ARN associado a uma mensagem de e-mail em trânsito.

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

Os campos alteráveis no exemplo anterior incluem o seguinte:

- Região — A região da AWS para sua WorkMail organização na Amazon.
- Conta — O Conta da AWS ID da sua WorkMail organização na Amazon.
- Organização — O ID da sua WorkMail organização na Amazon.
- Contexto – Indica se a mensagem é de `incoming` ou de `outgoing` da sua organização.
- ID da mensagem – O ID exclusivo da mensagem de e-mail que é transmitido como entrada para a função do Lambda.

O exemplo a seguir inclui IDs de exemplo para um ARN associado a uma mensagem de e-mail recebida em trânsito.

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

Você pode usar esses ARNs como recursos na `Resource` seção de suas políticas de usuário do IAM para gerenciar o acesso às WorkMail mensagens da Amazon em trânsito.

Exemplo de políticas do IAM para acesso ao fluxo de WorkMail mensagens da Amazon

O exemplo de política a seguir concede a uma entidade do IAM acesso total de leitura a todas as mensagens de entrada e saída de cada WorkMail organização da Amazon em sua. Conta da AWS

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

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

Se você tiver várias organizações em sua Conta da AWS, também poderá limitar o acesso a uma ou mais organizações. Isso é útil se determinadas funções do Lambda só puderem ser usadas para determinadas organizações.

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

Você também pode optar por conceder acesso a mensagens, dependendo de elas serem de `incoming` ou de `outgoing` na organização. Para fazer isso, use o qualificador `incoming` ou `outgoing` no ARN.

O exemplo de política a seguir concede acesso somente a mensagens de incoming (recebidas) na organização.

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

```
    ]
}
```

O exemplo de política a seguir concede a uma entidade do IAM acesso total de leitura e atualização a todas as mensagens de entrada e saída de cada WorkMail organização da Amazon em sua. Contas da AWS

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

Testar uma regra de fluxo de e-mail

Para verificar a configuração atual da regra, é possível testar como ela se comportará com endereços de e-mail específicos.

Para testar uma regra de fluxo de e-mail

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Organization setting (Configuração de organização) e Inbound/Outbound rules (Regras de recebimento/envio).
4. Ao lado de Test configuration (Testar configuração), insira os endereços de e-mail completos do remetente e do destinatário a serem testados.
5. Escolha Test (Testar). A ação a ser realizada no endereço de e-mail fornecido é exibida.

Remover uma regra de fluxo de e-mail

Ao remover uma regra de fluxo de e-mail, as alterações são aplicadas imediatamente.

Para remover uma regra de fluxo de e-mail

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Organization setting (Configuração de organização) e Inbound/Outbound rules (Regras de recebimento/envio).
4. Selecione a regra e escolha Remove.
5. No diálogo de confirmação, selecione Remove (Remover).

Aplicar políticas DMARC em e-mails recebidos

Domínios de e-mail usam registros de Sistema de Nomes de Domínio (DNS) para fins de segurança. Eles protegem seus usuários contra ataques comuns, como falsificação ou phishing. Os registros de DNS geralmente incluem registros de autenticação, relatórios e conformidade (DMARC) baseados em domínio, que são definidos pelo proprietário do domínio que envia o e-mail. Os registros DMARC incluem políticas que especificam ações a serem executadas quando um e-mail falhar em uma verificação de DMARC. Você pode escolher se deseja aplicar a política DMARC em e-mails enviados para sua organização.

Novas WorkMail organizações da Amazon têm a aplicação do DMARC ativada por padrão.

Como ativar a aplicação de DMARC

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, selecione Organization settings (Configurações da organização). A página de Configurações da organização será exibida, mostrando um conjunto de guias.
4. Selecione a guia DMARC e escolha Editar.
5. Mova o controle deslizante Aplicação de DMARC para a posição ativada.
6. Marque a caixa de seleção ao lado de Eu reconheço que ativar a aplicação do DMARC pode resultar na eliminação ou quarentena de e-mails recebidos com base na configuração do domínio do remetente.
7. Escolha Salvar.

Como desativar a aplicação de DMARC

- Siga as etapas da seção anterior, mas mova o controle deslizante Aplicação de DMARC para a posição desativada.

Usar o registro de eventos de e-mail em log para rastrear a aplicação de DMARC

A ativação da aplicação de DMARC pode resultar em e-mails recebidos serem descartados ou marcados como spam, dependendo de como o remetente configurou seu domínio. Se um remetente configurar incorretamente o domínio de e-mail, seus usuários poderão parar de receber e-mails legítimos. Para verificar se há e-mails que não estão sendo entregues aos seus usuários, você pode ativar o registro de eventos de e-mail para sua WorkMail organização Amazon. Depois, você pode consultar os logs de eventos para e-mails de entrada que são filtrados com base nas políticas DMARC do remetente.

Antes de usar o registro de eventos de e-mail para rastrear a aplicação do DMARC, habilite o registro de eventos de e-mail no console da Amazon WorkMail . Para obter o máximo de seus dados de log, aguarde enquanto os eventos de e-mail são registrados. Para mais informações e instruções, consulte the section called “Ativar o registro em log de eventos de e-mail”.

Como usar o registro de eventos de e-mail em log a fim de controlar a aplicação de DMARC

1. No console do CloudWatch Insights, em Logs, escolha Insights.
2. Em Selecionar grupo (s) de registros, selecione o grupo de registros da sua WorkMail organização Amazon. Por exemplo, /aws/workmail/events/organization-alias.

3. Selecione um período a ser consultado.
4. Execute a seguinte consulta: stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. Selecione Executar consulta.

Você também pode configurar métricas personalizadas para esses eventos. Para obter mais informações, consulte Criar filtros de métrica.

Marcar uma organização

Marcar um recurso WorkMail organizacional da Amazon permite que você:

- Diferencie entre organizações no console do AWS Billing and Cost Management.
- Controle o acesso aos recursos WorkMail da organização da Amazon adicionando-os ao `Resource` elemento das declarações de política de permissão AWS Identity and Access Management (IAM).

Para obter mais informações sobre as permissões em WorkMail nível de recursos da Amazon, consulte. Recursos Para obter mais informações sobre como controlar o acesso com base em tags, consulte Autorização baseada em WorkMail tags da Amazon.

WorkMail Os administradores da Amazon podem marcar organizações usando o WorkMail console da Amazon.

Para adicionar tags a uma WorkMail organização da Amazon

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Tags.
4. Em Organization tags (Tags da organização), escolha Add new tag (Adicionar nova tag).
5. Em Chave, insira um nome que identifique a marcação.

6. (Opcional) Em Value (Valor), insira um valor para a tag.
7. (Opcional) Repita as etapas 4 a 6 para adicionar mais tags à sua organização. É possível adicionar até 50 tags.
8. Escolha Salvar para salvar as alterações.

Você pode ver as tags da sua organização no WorkMail console da Amazon.

Os desenvolvedores também podem marcar organizações usando o AWS SDK ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte os `UntagResource` comandos`TagResource`,`ListTagsForResource`, e na Amazon WorkMail API Reference ou na AWS CLICommand Reference.

Você pode remover tags de uma organização a qualquer momento usando o WorkMail console da Amazon.

Para remover tags de uma WorkMail organização da Amazon

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Tags.
4. Em Organization tags (Tags da organização), escolha Remove (Remover) ao lado da tag a ser removida.
5. Escolha Submit (Enviar) para salvar as alterações.

Trabalhar com regras de controle de acesso

As regras de controle de acesso da Amazon WorkMail permitem que os administradores controlem como os usuários e as funções de personificação de sua organização recebem acesso à Amazon. WorkMail Cada WorkMail organização da Amazon tem uma regra de controle de acesso padrão que concede acesso à caixa de correio a todos os usuários e funções de representação adicionadas à organização, independentemente do protocolo de acesso ou endereço IP que eles usem. Os

administradores podem editar ou substituir a regra padrão por uma própria, adicionar uma nova regra ou excluir uma regra.

> **Warning**
>
> Se um administrador excluir todas as regras de controle de acesso de uma organização, a Amazon WorkMail bloqueará todo o acesso às caixas de correio da organização.

Os administradores podem aplicar regras de controle de acesso que permitem ou negam acesso com base nos seguintes critérios:

- Protocolos – O protocolo usado para acessar a caixa de correio. Os exemplos incluem Descoberta Automática, EWS, IMAP, SMTP ActiveSync, Outlook para Windows e Webmail.
- Endereços IP – Os intervalos CIDR IPv4 usados para acessar a caixa de correio.
- WorkMail Usuários da Amazon — Os usuários da sua organização que são usados para acessar a caixa de correio.
- Funções de personificação – As funções de personificação na organização usadas para acessar a caixa de correio. Para ter mais informações, consulte Gerenciamento de funções de personificação.

Os administradores aplicam regras de controle de acesso além das permissões de pasta e caixa de correio do usuário. Para obter mais informações, consulte Trabalhar com permissões de caixa de correio Compartilhamento de pastas e permissões de pastas no Guia WorkMail do usuário da Amazon.

> **Note**
>
> - Ao habilitar o acesso para o Outlook para Windows, recomanda-se habilitar também o acesso para Descoberta Automática e EWS.
> - As regras de controle de acesso não se aplicam ao WorkMail console da Amazon ou ao acesso ao SDK. Em vez disso, use políticas ou perfis do AWS Identity and Access Management (IAM). Para ter mais informações, consulte Gerenciamento de identidade e acesso para a Amazon WorkMail.

Criar regras de controle de acesso

Crie novas regras de controle de acesso no WorkMail console da Amazon.

Como criar uma regra de controle de acesso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Access control rules (Regras de controle de acesso).
4. Escolha a opção Criar regra.
5. Em Description (Descrição), insira uma descrição para a regra.
6. Em Effect (Efeito), escolha Allow (Permitir) ou Deny (Negar). Isso permite ou nega o acesso com base nas condições selecionadas na etapa a seguir.
7. Em Esta regra aplica-se a solicitações que…, selecione as condições a serem aplicadas à regra, como incluir ou excluir protocolos específicos, endereços IP ou ainda usuários ou funções de personificação.
8. (Opcional) Se você inserir intervalos de endereços IP, usuários ou funções de personificação, escolha Adicionar para adicioná-los à regra.
9. Escolha a opção Criar regra.

Editar regras de controle de acesso

Edite as regras de controle de acesso novas e padrão no WorkMail console da Amazon.

Como editar uma regra de controle de acesso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Access control rules (Regras de controle de acesso).
4. Selecione a regra a ser editada.
5. Selecione Edit rule.
6. Edite a descrição, o efeito e as condições, conforme necessário.
7. Escolha Salvar alterações.

> **Important**
>
> Quando você altera uma regra de acesso, as caixas de correio afetadas podem levar cinco minutos para seguir a regra atualizada. Os clientes que acessam as caixas de correio afetadas podem apresentar um comportamento inconsistente durante esse período. No entanto, você percebe imediatamente o comportamento correto ao testar as regras. Para obter mais informações sobre teste de regras, confira as etapas na próxima seção.

Testar regras de controle de acesso

Para ver como as regras de controle de acesso da sua organização são aplicadas, teste as regras no WorkMail console da Amazon.

Como testar regras de controle de acesso para sua organização

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Access control rules (Regras de controle de acesso).
4. Escolha Teste rules (Testar regras).
5. Em Request context (Contexto de solicitação), selecione o protocolo para o qual testar.
6. Em Source IP address (Endereço IP de origem), digite o endereço IP para o qual testar.

7. Em Solicitação realizada por, escolha Usuário ou Função de personificação para testar.
8. Selecione Usuário ou Função de personificação para testar.
9. Escolha Test (Testar).

Os resultados do teste são exibidos em Effect (Efeito).

Excluir regras de controle de acesso

Exclua as regras de controle de acesso que você não precisa mais do WorkMail console da Amazon.

> **Warning**
>
> Se um administrador excluir todas as regras de controle de acesso de uma organização, a Amazon WorkMail bloqueará todo o acesso às caixas de correio da organização.

Como excluir uma regra de controle de acesso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Access control rules (Regras de controle de acesso).
4. Selecione a regra a ser excluída.
5. Escolha Delete rule (Excluir regra).
6. Escolha Excluir.

Definir políticas de retenção de caixa postal

Você pode definir políticas de retenção de caixas de correio para sua WorkMail organização Amazon. As políticas de retenção excluem automaticamente mensagens de e-mail das caixas de correio de usuários após um período determinado por você. Você pode escolher em quais pastas de caixa de correio aplicar políticas de retenção. Além disso, você pode escolher se deseja definir

políticas de retenção diferentes para pastas diferentes. As políticas de retenção de caixa postal se aplicam às pastas selecionadas em todas as caixas postais do usuário em sua organização. Os usuários não podem substituir as políticas de retenção.

Como definir uma política de retenção de caixa postal

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Selecione Política de retenção.
4. Em Ações de pasta, ao lado de cada pasta da caixa postal que você deseja incluir na política, selecione Excluir ou Excluir permanentemente.
5. Insira o número de dias que as mensagens de e-mail de cada pasta da caixa de correio serão mantidas antes de serem excluídas.
6. Escolha Salvar.

Pode levar até 48 horas para as políticas de retenção da organização serem aplicadas. Se você escolher a ação Excluir pasta, os usuários poderão recuperar mensagens de e-mail excluídas do aplicativo WorkMail web da Amazon e dos clientes compatíveis. Se você escolher a ação Excluir permanentemente a pasta, os e-mails não poderão ser recuperados após serem excluídos.

O número de dias em que uma política de retenção mantém um item é baseado em quando ele foi criado, modificado ou movido. Por exemplo, se uma política de retenção exclui itens após um ano, a política contará os dias de retenção a partir da data em que você criou ou realizou a última ação nesse item. Ela não é afetada pela data em que você implementou a política de retenção.

Trabalhar com domínios

Você pode configurar WorkMail a Amazon para usar um domínio personalizado. Você também pode tornar um domínio o padrão para sua organização e habilitá-lo AutoDiscover para o Microsoft Outlook.

Tópicos

Adicionar um domínio

Você pode adicionar até 100 domínios à sua WorkMail organização Amazon. Ao adicionar um novo domínio, uma política de autorização de envio do Amazon Simple Email Service (Amazon SES) é adicionada automaticamente à política de identidade do domínio. Isso fornece à Amazon WorkMail acesso a todas as ações de envio do Amazon SES para seu domínio e permite que você redirecione e-mails para seu domínio. Você também pode redirecionar e-mails para domínios externos.

> **Note**
>
> Como prática recomendada, você deve adicionar aliases para `<postmaster@>` e `<abuse@>` para todos os seus domínios. É possível criar grupos de distribuição para esses aliases se você quiser que determinados usuários da sua organização recebam os e-mails enviados para esses aliases.

Ao configurar sua WorkMail organização Amazon com um domínio personalizado, lembre-se do seguinte sobre os registros DNS do seu domínio:

- Para registros MX e CNAME de descoberta automática, recomendamos definir o valor de Time to Live (TTL) como 3600. A redução do TTL garante que seus servidores de e-mail não usem registros MX desatualizados ou inválidos após a atualização desses registros ou a migração das suas caixas de correio.
- Depois de criar seus usuários e grupos de distribuição e migrar com sucesso suas caixas de correio, você deve atualizar o registro MX para começar a encaminhar e-mails para a Amazon. WorkMail As atualizações para registros de DNS podem levar até 48 horas para serem processadas.
- Alguns provedores de DNS anexam automaticamente nomes de domínio ao final dos registros DNS. Adicionar um registro que já contenha o nome de domínio, como _amazonses.example.com, pode resultar na duplicação do nome de domínio, resultando em _amazonses.example.com.example.com. Para evitar a duplicação do nome do domínio no nome de registro, adicione um ponto ao final do nome do domínio no registro DNS. Isso indica ao seu provedor de DNS que o nome de registro está totalmente qualificado, não sendo mais relativo ao nome do domínio. Isso também impede que o provedor de DNS adicione mais um nome de domínio.
- Os nomes de registro que são copiados incluem o nome do domínio. Dependendo serviço de DNS usado, talvez o nome do domínio já esteja adicionado ao registro de DNS do domínio.
- Depois de criar um registro DNS, escolha o ícone de atualização no WorkMail console da Amazon para ver o status da verificação e o valor do registro. Para obter mais informações sobre como verificar domínios, consulte Verificar domínios.
- Recomendamos que você configure seu domínio como o domínio `MAIL FROM`. Para habilitar AutoDiscover para dispositivos iOS, você deve configurar seu domínio como o `MAIL FROM` domínio. Você pode ver o status do seu domínio `MAIL FROM` na seção Melhorar a capacidade de entrega do console. Para obter mais informações, consulte Configurar um domínio MAIL FROM personalizado.

Para adicionar um domínio

1. Faça login no AWS Management Console e abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

2. Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
3. No painel de navegação, escolha Organizações e, em seguida, selecione o nome da organização à qual você deseja adicionar um domínio.
4. No painel de navegação, escolha Domínios e, em seguida, Adicionar Domínio.
5. Na tela Adicionar domínio, insira um nome de domínio. Os nomes de domínio podem conter apenas caracteres latinos básicos (ASCII).

   > **Note**
   >
   > Se houver um domínio gerenciado em uma zona hospedada pública do Amazon Route 53, ele pode ser selecionado no menu suspenso que é exibido quando o nome do domínio é inserido.

6. Escolha Adicionar domínio.

   Uma página é exibida e relaciona os registros de DNS do novo domínio. A página agrupa os registros nas seguintes seções:

   - Propriedade do domínio
   - WorkMail configuração
   - Segurança aprimorada
   - Entrega de e-mail aprimorada

   Cada uma dessas seções contém um ou mais registros de DNS, e cada registro exibe um valor de Status. A lista a seguir mostra os registros com os valores de status disponíveis.

   Propriedade do TXT

   Verificado – Registro resolvido e verificado.

   Pendente – Registro ainda não verificado.

   Falha – Não foi possível verificar a propriedade. Registro sem correspondência ou inacessível.

Configuração MX WorkMail

Verificado – Registro resolvido e verificado.

Ausente – Não foi possível resolver o registro.

Inconsistente – O valor não corresponde ao registro esperado.

AutoDiscover

Verificado – Registro resolvido e verificado.

Ausente – Não foi possível resolver o registro.

Inconsistente – O valor não corresponde ao registro esperado.

> **Note**
>
> O processo AutoDiscover de verificação também verifica a AutoDiscover configuração correta. O processo verifica as configurações de cada fase. Uma marca de seleção verde aparece ao lado de Verificado na coluna Status quando a verificação é concluída. Você pode passar o mouse sobre Verificado e ver quais das fases foram verificadas pelo processo. Para obter mais informações sobre as AutoDiscover fases, consulteHabilitando AutoDiscover a configuração de endpoints.

DKIM CNAME

Verificado – Registro resolvido e verificado.

Pendente — Registro ainda não verificado

Falha – Não foi possível verificar a propriedade. Registro sem correspondência ou inacessível.

Para obter mais informações sobre assinatura DKIM, consulte Autenticar e-mail com DKIM no Amazon SES na Guia do desenvolvedor do Amazon Simple Email Service.

SPF TXT

Verificado – Registro resolvido e verificado.

Ausente – Não foi possível resolver o registro.

Inconsistente – O valor não corresponde ao registro esperado.

Para obter mais informações sobre verificação de SPF, consulte Autenticar e-mail com SPF.

DMARC TXT

Verificado – Registro resolvido e verificado.

Ausente – Não foi possível resolver o registro.

Inconsistente – O valor não corresponde ao registro esperado

Para obter mais informações sobre registros DMARC na Amazon WorkMail, consulte Conformidade com o DMARC usando o Amazon SES no Guia do desenvolvedor do Amazon Simple Email Service.

Domínio TXT MAIL FROM

Verificado – Registro resolvido e verificado.

Pendente – Registro ainda não verificado.

Falha – Não foi possível verificar a propriedade. Registro sem correspondência ou inacessível.

Domínio MX MAIL FROM

Verificado – Registro resolvido e verificado.

Ausente – Não foi possível resolver o registro.

Inconsistente – O valor não corresponde ao registro esperado.

7. Para a próxima etapa, escolha a ação apropriada com base no provedor de DNS que você usa.

Se você usa um domínio do Route 53

- Na parte superior da página, escolha Atualizar tudo no Route 53.

Se você usa outro provedor de DNS

- Copie os registros e cole-os no seu provedor de DNS. Você pode copiar os registros em massa ou um de cada vez. Para copiar registros em massa, escolha Copiar tudo. Isso cria uma zona de arquivo que você pode importar para o seu provedor de DNS. Para copiar registros um de cada vez, escolha os quadrados sobrepostos ao lado do nome do registro e cole cada um no seu provedor de DNS.

8. Escolha o ícone de atualização para atualizar o Status de cada registro. Isso verifica a propriedade do domínio e a configuração adequada do seu domínio com a Amazon WorkMail.

Remover um domínio

Quando você não precisar mais de um domínio, é possível excluí-lo. No entanto, primeiro você deve excluir todos os indivíduos ou grupos que usam o domínio como endereço de e-mail.

Para remover um domínio

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Nome de regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizações e, em seguida, selecione o nome da organização.
3. Na lista de domínios, marque a caixa de seleção ao lado do nome de domínio e escolha Remove.
4. Na caixa de diálogo Remove domain, digite o nome do domínio a ser removido e escolha Remove.

Escolher o domínio padrão

Você pode tornar um domínio associado à sua organização padrão para usuários e grupos nessa organização. Tornar um domínio padrão não altera os endereços de e-mail existentes.

Para tornar um domínio padrão

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Nome de regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizações e, em seguida, selecione o nome da organização.
3. Na lista de domínios, marque a caixa de seleção ao lado do nome do domínio e escolha Definir como padrão.

Verificar domínios

Você deve verificar seu domínio depois de adicioná-lo ao WorkMail console da Amazon. A verificação do domínio confirma que você é o proprietário do domínio e usará a Amazon WorkMail como serviço de e-mail para o domínio.

Você verifica um domínio adicionando registros TXT e MX a ele no seu serviço de DNS. Os registros TXT permitem que você adicione notas ao seu serviço de DNS. Os registros MX especificam o servidor de e-mail de entrada.

Você usa o console do Amazon SES para criar os registros TXT e MX e, em seguida, usa o WorkMail console da Amazon para adicionar os registros ao seu serviço DNS. Siga estas etapas.

Para criar registros TXT e MX

1. Faça login no Amazon SES em https://console.aws.amazon.com/ses/.
2. No painel de navegação, escolha Domínios e, em seguida, Verificar um novo domínio.

   A caixa de diálogo Verificar um novo domínio é exibida.
3. Na caixa Domínio, insira o nome do domínio que você criou na seção Adicionar um domínio.
4. (Opcional) Se você quiser usar Correio DomainKeys Identificado (DKIM), marque a caixa de seleção Gerar configurações de DKIM.
5. Escolha Verificar esse domínio.

   O console exibe uma lista de registros TXT e MX.

6. Escolha o link Download Record Set as CSV, localizado abaixo da lista TXT.

   A caixa de diálogo Salvar como é exibida. Escolha um local para fazer o download e, em seguida, escolha Salvar.

7. Abra o arquivo CSV baixado e copie todo o seu conteúdo.

Depois de criar os registros TXT e MX, você os adiciona ao seu provedor de DNS. As etapas a seguir usam o Route 53. Se você usa um provedor de DNS diferente e não sabe como adicionar registros, consulte a documentação do seu provedor.

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas. Em seguida, escolha o botão de opção ao lado do domínio que você deseja verificar.
3. Na lista de registros DNS do seu domínio, escolha Importar arquivo de zona.
4. Em Arquivo de zona, cole os registros copiados na caixa de texto. Uma lista dos arquivos é exibida abaixo da caixa de texto.
5. Desça até o final da lista e escolha Importar.

> **Note**
>
> Aguarde até 72 horas para concluir o processo de verificação.

Verificar registros TXT e MX com o serviço de DNS

Confirme se o registro TXT que verifica se você possui o domínio está adicionado corretamente ao serviço de DNS. Este procedimento usa a ferramenta nslookup, que está disponível para Windows e Linux. No Linux, você também pode usar dig.

Para usar a ferramenta `nslookup`, você primeiro encontra os servidores de DNS que atendem ao seu domínio. Em seguida, você consulta esses servidores para visualizar os registros TXT. Você pode consultar os servidores DNS do seu domínio porque esses servidores contêm a maioria das up-to-date informações do seu domínio. Essas informações pode levar algum tempo para serem propagadas para outros servidores de DNS.

Para usar o nslookup para verificar se o registro TXT está adicionado ao serviço de DNS

1. Encontre os servidores de nomes do seu domínio:

   a. Abra um prompt de comando (Windows) ou terminal (Linux).

   b. Execute o comando a seguir para listar todos os servidores de nome que atendem ao seu domínio. Substitua *example.com* pelo seu domínio.

   ```
   nslookup -type=NS example.com
   ```

   Você poderá consultar um desses servidores na próxima etapa.

2. Verifique se o registro WorkMail TXT da Amazon foi adicionado corretamente.

   a. Execute o comando a seguir, substituindo *example.com* pelo seu domínio e *ns1.name-server.net* por um servidor de nomes da Etapa 1.

   ```
   nslookup -type=TXT _amazonses.example.com ns1.name-server.net
   ```

   b. Analise a `"text ="` string mostrada na saída de nslookup. Confirme se essa string corresponde ao valor de TXT do seu domínio na lista de remetentes verificados no console da Amazon WorkMail.

   No exemplo a seguir, procure por um registro TXT em _amazonses.example.com com o valor de `fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk=`. Se o registro estiver atualizado corretamente, o comando deverá ter a seguinte saída:

   ```
   _amazonses.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
   ```

Para usar dig para verificar se o registro TXT está adicionado ao serviço de DNS

1. Abra uma sessão do terminal.
2. Execute o comando a seguir para listar os registros TXT para o seu domínio. Substitua *example.com* pelo seu domínio.

   ```
   dig +short example.com txt
   ```

3. Verifique se a sequência de caracteres que segue TXT na saída do comando corresponde ao valor de TXT que você vê ao selecionar o domínio na lista de remetentes verificados do console da Amazon WorkMail.

Para usar nslookup para verificar se o registro MX está adicionado ao serviço de DNS

1. Encontre os servidores de nome do seu domínio:

   a. Abra um prompt de comando.

   b. Execute o comando a seguir para listar todos os servidores de nome que atendem ao seu domínio.

   ```
   nslookup -type=NS example.com
   ```

   Você poderá consultar um desses servidores de nome na próxima etapa.

2. Verifique se o registro MX foi adicionado corretamente:

   a. Execute o comando a seguir, substituindo *example.com* pelo seu domínio e *ns1.name-server.net* por um dos servidores de nome identificados na etapa anterior.

   ```
   nslookup -type=MX example.com ns1.name-server.net
   ```

   b. Na saída do comando, verifique se a string após `mail exchange =` corresponde a um dos valores a seguir:

   Região Leste dos EUA (N. da Virgínia) – `10 inbound-smtp.us-east-1.amazonaws.com`

   Região Oeste dos EUA (Oregon) – `10 inbound-smtp.us-west-2.amazonaws.com`

   Região Europa (Irlanda) – `10 inbound-smtp.eu-west-1.amazonaws.com`

   > **Note**
   >
   > `10` representa o número ou a prioridade de preferência de MX.

Para usar dig para verificar se o registro MX está adicionado ao serviço de DNS

1. Abra uma sessão do terminal.
2. Execute o comando a seguir para listar os registros MX para seu domínio.

```
dig +short example.com mx
```

3. Verifique se a string após `MX` corresponde a um dos seguintes valores:

   Região Leste dos EUA (N. da Virgínia) – `10 inbound-smtp.us-east-1.amazonaws.com`

   Região Oeste dos EUA (Oregon) – `10 inbound-smtp.us-west-2.amazonaws.com`

   Região Europa (Irlanda) – `10 inbound-smtp.eu-west-1.amazonaws.com`

   > **Note**
   >
   > `10` representa o número ou a prioridade de preferência de MX.

Solucionar problemas de verificação de domínio

Para solucionar problemas comuns com a verificação de domínio, verifique as sugestões a seguir:

Seu provedor de DNS não permite sublinhados em nomes de registro TXT

Omitir `_amazonses` do nome do registro TXT.

Você deseja verificar o mesmo domínio várias vezes, mas não pode ter vários registros TXT com o mesmo nome

Se o seu serviço de DNS não permite que você tenha vários registros TXT com o mesmo nome, use uma das soluções a seguir:

- (Recomendado) Se o serviço de DNS permitir, atribua vários valores ao registro TXT. Por exemplo, se o DNS for gerenciado pelo Amazon Route 53, você poderá configurar vários valores para o mesmo registro TXT da seguinte forma:
  1. No console do Route 53, escolha o registro TXT `_amazonses` que você adicionou ao verificar seu domínio na primeira região.
  2. Em Value (Valor), pressione Enter após o primeiro valor.
  3. Adicione o valor para a região adicional e salve o conjunto de registros.

- Se você precisa verificar seu domínio apenas duas vezes, poderá verificá-lo uma vez criando um registro TXT com `_amazonses` no nome e, depois, criando outro registro sem `_amazonses` no nome do registro.

O WorkMail console da Amazon relata que a verificação do domínio falhou

A Amazon não WorkMail consegue encontrar o registro TXT necessário para seu serviço de DNS. Verifique se o registro TXT necessário está adicionado corretamente ao servidor de DNS seguindo o procedimento em Verificar registros TXT e MX com o serviço de DNS.

Seu provedor de DNS acrescentou o nome do domínio ao final do registro TXT

Adicionar um registro que já contenha o nome de domínio, como _amazonses.example.com, pode resultar na duplicação de nome do domínio como _amazonses.example.com.example.com. Para evitar a duplicação do nome do domínio no nome de registro, adicione um ponto ao final do nome do domínio no registro TXT. Isso indica ao seu provedor de DNS que o nome do registro está totalmente qualificado e já tem o nome de domínio incluído no registro TXT.

A Amazon WorkMail relata que o registro MX é inconsistente

Ao migrar de servidores de e-mail existentes, o registro MX pode retornar um status de Inconsistente. Atualize seu registro MX para apontar para a Amazon WorkMail em vez de apontar para o servidor de e-mail anterior. O registro MX também é retornado como inconsistente quando um proxy de e-mail de terceiros é usado junto com a Amazon. WorkMail Se esse for o caso, é seguro ignorar o aviso de Inconsistente.

Habilitando AutoDiscover a configuração de endpoints

AutoDiscover permite que você configure o Microsoft Outlook e clientes móveis usando somente seu endereço de e-mail e senha. O serviço mantém uma conexão com a Amazon WorkMail e atualiza as configurações locais sempre que você altera os endpoints ou as configurações. Além disso, AutoDiscover permite que seu cliente use WorkMail recursos adicionais da Amazon, como o Catálogo de Endereços Offline, o Assistente de Ausência Temporária e a capacidade de visualizar o horário livre/ocupado no Calendário.

O cliente executa as seguintes AutoDiscover fases para detectar os URLs do endpoint do servidor:

- Fase 1: o cliente realiza uma consulta de Secure Copy Protocol (SCP) no Active Directory local. Se seu cliente não estiver associado ao domínio, AutoDiscover pule esta etapa.

- Fase 2: o cliente envia uma solicitação para as URLs a seguir e valida os resultados. Esses endpoints só estão disponíveis usando HTTPS.
  - https://*company.tld*/autodiscover/autodiscover.xml
  - https://autodiscover.*company.tld*/autodiscover/autodiscover.xml
- Fase 3: o cliente realiza uma consulta de DNS em autodiscover.company.tld e envia uma solicitação GET não autenticada ao endpoint derivado do endereço de e-mail do usuário. Se o servidor retornar um redirecionamento 302, o cliente reenviará a AutoDiscover solicitação para o endpoint HTTPS retornado.

Se ocorrer falha em todas essas fases, o cliente não poderá ser configurado automaticamente. Para obter informações sobre como configurar manualmente dispositivos móveis, consulte Conectar seu dispositivo manualmente.

Você será solicitado a adicionar o registro AutoDiscover DNS ao seu provedor ao adicionar seu domínio à Amazon. WorkMail Isso permite que o cliente execute a fase 3 do AutoDiscover processo. No entanto, essas etapas não funcionam em todos os dispositivos móveis, como o aplicativo de e-mail nativo do Android. Como resultado, talvez seja necessário configurar a AutoDiscover fase 2 manualmente.

Você pode usar os seguintes métodos para configurar a AutoDiscover fase 2 para seu domínio:

(Recomendado) Use o Route 53 e a Amazon CloudFront

> **Note**
>
> As etapas a seguir mostram como criar um proxy para https://autodiscover.*company.tld*/autodiscover/autodiscover.xml. Para usar proxy em https://*company.tld*/autodiscover/autodiscover.xml, remova o prefixo `autodiscover.` dos domínios nas etapas a seguir.
> O uso CloudFront do Route 53 pode acarretar custos. Para obter mais informações sobre os preços aplicáveis, consulte os CloudFront preços da Amazon e os preços do Amazon Route 53.

Para habilitar a AutoDiscover fase 2 com o Route 53 e CloudFront

1. Obtenha um certificado SSL para autodiscover.*company.tld* e faça upload dele no AWS Identity and Access Management (IAM) ou no AWS Certificate Manager. Para obter mais

informações, consulte Trabalhar com certificados de servidor no Guia de usuário do IAM ou Conceitos básicos no Guia de usuário do AWS Certificate Manager.

2. Crie uma nova CloudFront distribuição:

   1. Abra o CloudFront console emhttps://console.aws.amazon.com/cloudfront/v4/home.
   2. No painel de navegação, escolha Distribuições.
   3. Escolha Criar distribuição.
   4. Em Web, selecione Conceitos básicos.
   5. Em Configurações de origem, insira os valores a seguir:
      - Nome do domínio de origem – O nome do domínio apropriado para sua região:
        - Leste dos EUA (Norte da Virgínia) – **`autodiscover-service.mail.us-east-1.awsapps.com`**
        - Oeste dos EUA (Oregon) – **`autodiscover-service.mail.us-west-2.awsapps.com`**
        - Europa (Irlanda) – **`autodiscover-service.mail.eu-west-1.awsapps.com`**
      - Política de protocolo de origem – A política desejada: **`Match Viewer`**

        > **Note**
        >
        > Deixe o Caminho de origem em branco. Não altere o valor preenchido automaticamente para o ID de origem.

   6. Em Configurações de comportamento do cache padrão, selecione os valores a seguir para as configurações listadas:
      - Viewer Protocol Policy: HTTPS Only
      - Allowed HTTP Methods: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
      - Cache baseado em cabeçalhos de solicitação selecionados: Todos
      - Forward Cookies: All
      - Encaminhamento e armazenamento de string de consulta em cache: Nenhum (Melhora o armazenamento em cache)
      - Smooth Streaming: No
      - Restrict Viewer Access: No
   7. Selecione os valores a seguir para Distribution Settings (Configurações de distribuição):

- Price Class: use apenas "US", "Canada" e "Europe"
- Para Nomes de domínio alternativos (CNAMEs), insira **`autodiscover.`*`company.tld`*** ou ***`company.tld`***, onde *`company.tld`* é seu nome de domínio.
- Certificado SSL: certificado SSL personalizado (armazenado no IAM)
- Custom SSL Client Support (Suporte ao cliente SSL personalizado): selecione All Clients (Todos os clientes) ou Only Clients that Support Server Name Indication (SNI) (Somente os clientes que oferecem suporte à indicação de nome de servidor (SNI)). As versões mais antigas do Android podem não funcionar com a última opção.

> **Note**
>
> Se você selecionar All Clients (Todos os clientes), deixe Default Root Object (Objeto raiz padrão) em branco.

- Logging (Registro em log): selecione On (Ativado) ou Off (Desativado). Ativado habilita o registro em log.
- Em Comment (Comentário), digite **`AutoDiscover type2 for autodiscover.`*`company.tld`***
- Em Estado de distribuição, selecione Habilitado.

8. Escolha Criar distribuição.

3. No console do Route 53, crie um registro que roteie o tráfego da Internet do seu nome de domínio para sua CloudFront distribuição.

> **Note**
>
> Essas etapas pressupõem que o registro de DNS de example.com está hospedado no Route 53. Se você não usa o Route 53, siga os procedimentos no console de gerenciamento do seu provedor de DNS.

1. No painel de navegação do console, selecione Zonas hospedadas e, em seguida, escolha um domínio.
2. Na lista de domínios, escolha o nome de domínio que você deseja usar.
3. Em Registros, escolha Criar registro.
4. Em Registro de criação rápida, defina os seguintes parâmetros:

- Em Nome do registro, insira um nome para o registro.
- Em Política de roteamento, selecione Roteamento simples.
- Escolha o controle deslizante Alias para ativá-lo. O controle deslizante fica azul quando está no estado ativado.
- Em Tipo de registro, escolha A - Encaminha o tráfego para um endereço IPv4 e alguns recursos da AWS.
- Na lista Rotear tráfego para, escolha Alias para CloudFront distribuição.
- Uma caixa de pesquisa aparecerá abaixo da lista Encaminhar tráfego para. Insira o nome da sua CloudFront distribuição na caixa de texto. Você também pode selecionar a distribuição na lista que aparece quando você seleciona a caixa de pesquisa.

5. Escolha Create record (Criar registro).

Para usar um servidor web Apache

As etapas a seguir explicam como usar um servidor web Apache para criar um proxy para https://autodiscover.*company.tld*/autodiscover/autodiscover.xml. Para criar um proxy para https://*company.tld*/autodiscover/autodiscover.xml, remova a "descoberta automática". prefixo dos domínios nas etapas a seguir.

Para habilitar a AutoDiscover fase 2 com um servidor web Apache

1. Execute as diretivas a seguir em um servidor Apache com SSL habilitado:

```
SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-
service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
```

2. Conforme necessário, habilite os seguintes módulos Apache. Se você não souber como, consulte a ajuda do Apache:

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`
   - `ssl`

Consulte a seção a seguir para obter informações sobre testes e solução de problemas AutoDiscover.

AutoDiscover solução de problemas da fase 2

Depois de configurar seu provedor de DNS para AutoDiscover, você pode testar a configuração do seu AutoDiscover endpoint. Se o endpoint do AutoDiscover estiver configurado corretamente, ele responde com uma mensagem de solicitação não autorizada.

Para fazer uma solicitação não autorizada básica

1. Em um terminal, crie uma solicitação POST não autenticada para o AutoDiscover endpoint.

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ```

   Se o endpoint estiver configurado corretamente, ele deverá retornar uma mensagem `401 unauthorized`, como mostrado no exemplo a seguir:

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ...
   HTTP/1.1 401 Unauthorized
   ```

2. Em seguida, teste uma AutoDiscover solicitação real. Crie um arquivo `request.xml` com o seguinte conteúdo 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. Use o `request.xml` arquivo que você criou e faça uma AutoDiscover solicitação autenticada para o endpoint. Lembre-se de substituir *`testuser@company.tld`* por um endereço de e-mail válido:

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

A resposta será semelhante à resposta do exemplo a seguir se o endpoint estiver configurado corretamente:

```
$ 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>
```

Editar políticas de identidade do domínio

As políticas de identidade de domínio especificam as permissões das ações de e-mail, como o redirecionamento de mensagens de e-mails. Por exemplo, você pode redirecionar e-mails para qualquer endereço de e-mail na sua WorkMail organização Amazon.

> **Note**
>
> A partir de 1º de abril de 2022, WorkMail a Amazon começou a usar diretores de serviços para autorização em vez de diretores de AWS conta. Se você adicionou um domínio antes de 1º de abril de 2022, talvez tenha uma política mais antiga que usa uma entidade principal de conta da AWS para autorização. Nesse caso, recomendamos atualizar para a política mais recente. As etapas nesta seção explicam como fazer isso. Sua organização continua enviando e-mails normalmente durante a atualização.

Você só segue essas etapas se não usar uma política personalizada do Amazon SES. Se você usa uma política personalizada do Amazon SES, você mesmo deve atualizá-la. Para obter mais informações, consulte Política de entidade principal de serviço personalizada do Amazon SES mais adiante neste tópico.

> **Important**
>
> Não remova seus domínios existentes. Se você fizer isso, você interromperá o serviço de correio. Tudo o que você precisa fazer é inserir novamente seus domínios existentes.

Para atualizar uma política de identidade de domínio

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Para fazer isso, abra a lista Selecionar uma região, localizada à direita da caixa de pesquisa, e escolha a região desejada. Para obter mais informações sobre as regiões, consulte Regiões e endpoints em Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizações e, em seguida, selecione o nome da organização.
3. No painel de navegação à esquerda, escolha Domínios.
4. Destaque e copie o nome do domínio que você deseja inserir novamente e selecione Adicionar domínio.

   A caixa de diálogo Adicionar domínio será exibida.
5. Cole o nome copiado na caixa Nome do domínio e escolha Adicionar domínio.

6. Repita as etapas de 3 a 5 para os domínios restantes em sua organização.

Política de entidade principal de serviço personalizada do Amazon SES

Se você usa uma política personalizada do Amazon SES, adapte esse exemplo para uso em seu domínio.

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

Autenticar e-mail com SPF

O Sender Policy Framework (SPF) é um padrão de confirmação de e-mails criado para combater a falsificação de e-mails. Falsificação é o ato de fazer com que um e-mail enviado por um agente mal-intencionado pareça com um enviado por um usuário legítimo. Para obter informações sobre como configurar o SPF para seu domínio WorkMail habilitado para Amazon, consulte Autenticação de e-mail com SPF no Amazon SES.

Configurar um domínio MAIL FROM personalizado

Por padrão, a Amazon WorkMail usa um subdomínio de amazonses.com como `MAIL FROM` domínio para seu e-mail de saída. Isso pode causar falha na entrega se a política DMARC em seu domínio estiver configurada apenas para SPF. Para resolver isso, configure seu próprio domínio como domínio `MAIL FROM`. Para saber como configurar seu domínio de e-mail como domínio `MAIL FROM`, consulte Configurar um domínio MAIL FROM personalizado no Guia do desenvolvedor do Amazon Simple Email Service.

> **Important**
>
> É necessário um domínio MAIL FROM personalizado quando você ativa AutoDiscover para dispositivos iOS.

Para obter mais informações sobre domínios `MAIL FROM` personalizados, consulte O Amazon SES agora oferece suporte a domínios MAIL FROM personalizados.

Trabalhar com usuários

Você pode criar e remover usuários da Amazon WorkMail. Além disso, você pode redefinir suas senhas de e-mail, gerenciar suas cotas de caixa de correio e acesso a dispositivos e controlar suas permissões de caixa de correio.

Tópicos

Visualizando uma lista de usuários

Para ver a lista de usuários

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da sua organização.
3. No painel de navegação, escolha Users.
4. Além disso, você pode filtrar usuários por nome de usuário, nome de exibição ou endereço de e-mail principal.

> **Note**
>
> A pesquisa diferencia maiúsculas de minúsculas.

Incluir um usuário

Quando você adiciona um usuário, a Amazon cria WorkMail automaticamente caixas de correio para ele. Os usuários podem fazer login e acessar seus e-mails a partir do aplicativo WorkMail web da Amazon, de seu dispositivo móvel ou usando o Microsoft Outlook no macOS ou PC.

Para adicionar um usuário

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização à qual você deseja adicionar usuários.
3. No painel de navegação, escolha Usuários e, em seguida, escolha Adicionar usuário.

   A tela Adicionar um usuário é exibida.
4. Em Detalhes do usuário, no campo Nome do usuário, insira o nome do usuário. O nome também aparece na caixa Endereço de e-mail. Se você quiser que o usuário tenha um endereço de e-mail diferente do nome de usuário, edite o campo Endereço de e-mail.
5. (Opcional) Insira o nome e o sobrenome do usuário nas caixas Nome e Sobrenome.
6. Na caixa Nome de exibição, insira o nome de exibição do usuário.
7. Na caixa Endereço de e-mail, aceite o alias de e-mail ou insira outro.
8. Por padrão, os usuários são exibidos na lista de endereços global. Para ocultar o usuário da lista de endereços global, desmarque a caixa de seleção Mostrar na lista de endereços global.
9. Selecione Usuário remoto para adicionar um usuário como usuário remoto à organização.
10. Em Configuração de senha, insira a senha do usuário nas caixas Senha e Repetir senha.
11. Escolha Adicionar usuário.

Como habilitar usuários

Quando você integra a Amazon WorkMail com seu Active Directory corporativo, ou você já tem usuários disponíveis em seu diretório Simple AD, você pode habilitar esses usuários na Amazon WorkMail. Você também segue estas etapas para reativar um usuário cuja conta foi desabilitada.

Para habilitar usuários

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e escolha a organização para a qual você deseja habilitar usuários.
3. No painel de navegação, escolha Users.

   Uma lista de usuários é exibida. As contas de usuário nos estados de usuário habilitado, desabilitado e do sistema são mostradas na lista.
4. Na lista de usuários com contas desativadas, marque as caixas de seleção dos usuários que você deseja habilitar e escolha Habilitar.

   A caixa de diálogo Habilitar usuários será exibida.
5. Conforme necessário, revise e altere o endereço de e-mail principal de cada usuário e escolha Habilitar.

Gerenciando aliases de usuário

Você pode adicionar ou remover aliases de e-mail para os usuários.

Para adicionar um alias de e-mail a um usuário

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da organização para a qual você deseja adicionar usuários.
3. No painel de navegação, escolha Usuários e selecione o nome do usuário ao qual você deseja adicionar um alias.
4. Na seção Detalhes do usuário, escolha a guia Aliases.
5. Na guia Aliases, escolha Adicionar alias.
6. Na caixa Alias, insira um alias.
7. Selecione um domínio para um alias.
8. Escolha Adicionar.

Para remover um alias de e-mail de um usuário

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da organização da qual você deseja remover usuários.
3. No painel de navegação, escolha Usuários e, em seguida, selecione o nome do usuário do qual você deseja remover aliases.
4. Na seção Detalhes do usuário, escolha a guia Aliases.
5. Na guia Aliases, marque a caixa de seleção dos aliases que você deseja remover.
6. Verifique os aliases que serão removidos.
7. Na janela Remover aliases, escolha Remover.

Desabilitar usuários

Você pode desativar qualquer usuário em uma organização a qualquer momento. Quando você desativa um usuário, ele fica imediatamente inacessível. Usuários desativados por mais de 30 dias terão suas caixas de entrada excluídas da Amazon WorkMail.

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, selecione Organizações e, em seguida, escolha a organização que contém os usuários que você deseja desabilitar.
3. No painel de navegação, escolha Users.

   Uma lista de todos os usuários é exibida, mostrando contas que estão nos estados habilitado, desabilitado e usuário do sistema.
4. Na lista de usuários habilitados, marque as caixas de seleção das contas que você deseja desabilitar e, em seguida, escolha Desativar.

   A caixa de diálogo Desabilitar usuários será exibida.
5. Escolha Disable.

Editar detalhes de usuários

Ao editar os detalhes do usuário, você pode alterar o seguinte:

- Dados pessoais — nomes, endereço de e-mail, números de telefone e outros detalhes pessoais.
- Cotas de caixa de correio (tamanhos): as cotas podem variar de 1 MB a 51.200 MB (50 GB). A Amazon WorkMail notifica os usuários quando eles atingem 90% de sua cota. Alterar a cota da caixa de correio de um usuário não afeta a definição de preços. Para obter mais informações sobre preços, consulte Amazon WorkMail Pricing.
- Acesso a dispositivos móveis: remova e limpe os dispositivos e visualize os detalhes do dispositivo.
- Permissões de acesso à caixa de correio: conceda aos usuários permissão para usar uma caixa de correio, além de diferentes níveis de acesso à caixa de correio.

> **Note**
>
> Se você integrar a Amazon WorkMail a um diretório do AD Connector, não poderá editar esses detalhes noAWS Management Console. Edite-os usando as ferramentas de gerenciamento do seu Active Directory. As limitações se aplicam quando a organização está

no modo de interoperabilidade. Para ter mais informações, consulte Limitações no modo de interoperabilidade.

Para editar os detalhes do usuário

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha a organização que você deseja usar.
3. No painel de navegação, selecione Usuários e, em seguida, escolha o nome do usuário a ser editado.

Para editar dados pessoais

1. Na seção Detalhes do usuário, escolha Editar.
2. Em Detalhes do usuário, insira ou altere as informações pessoais do usuário conforme necessário.
3. Ao concluir, escolha Salvar alterações.

Para editar cotas de caixa de correio

1. Em Detalhes do usuário, selecione a guia Cota e escolha Editar.
2. Na caixa Atualizar cota da caixa de correio, insira um tamanho para a caixa de correio. Você pode inserir valores de **1** a **51200**.
3. Escolha Salvar alterações.

Para gerenciar dados de dispositivos móveis

> **Note**
>
> Para gerenciar dispositivos móveis, seus usuários precisam primeiro conectar seus dispositivos à sua instância da Amazon WorkMail. Para obter informações sobre como

conectar dispositivos móveis, consulte Configurar clientes de dispositivos móveis para a Amazon WorkMail.

1. Em Detalhes do usuário, escolha a guia Dispositivos móveis.
2. Para ver uma lista atual de dispositivos, escolha Atualizar.
3. Para ver os detalhes de um dispositivo, escolha o nome do dispositivo na coluna ID do dispositivo.
4. Para remover ou apagar o dispositivo, selecione o botão de opção ao lado do nome do dispositivo e, em seguida, escolha Remover ou Apagar, conforme necessário.
5. Na caixa de diálogo exibida, confirme a operação de remoção ou limpeza. Lembre-se de que os usuários reaparecerão quando sincronizarem seus dispositivos com a Amazon WorkMail novamente.

Para editar permissões de caixa de correio

1. Escolha a aba Permissões.
2. Faça um dos seguintes procedimentos:

    1. Para adicionar permissões, escolha Adicionar permissões. Abra a lista Adicionar novas permissões e escolha um usuário ou grupo, escolha as configurações de permissão para o usuário ou grupo e selecione Salvar.
    2. Para editar as permissões do usuário, escolha o botão ao lado do nome do usuário. Escolha Editar, selecione as opções desejadas e escolha Salvar.

    Para obter mais informações sobre as opções de permissão, consulte Trabalhar com permissões de caixa de correio.
3. Para remover todas as permissões, escolha Remover e confirme a remoção.

Redefinindo a senha do usuário

Se um usuário esquecer sua senha ou tiver problemas para fazer login na Amazon WorkMail, você poderá redefinir a senha.

> **Note**
>
> Se você integrou a Amazon WorkMail a um diretório do AD Connector, deverá redefinir a senha do usuário no Active Directory.

Para redefinir uma senha do usuário

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Users.
4. Na lista de usuários, marque a caixa de seleção ao lado do nome do usuário e escolha Redefinir senha.
5. Na caixa de diálogo Redefinir senha, insira a nova senha e escolha Redefinir.

Solução de problemas de políticas de WorkMail senha da Amazon

Se a redefinição de senha não for bem-sucedida, verifique se a nova senha atende aos requisitos da política de senhas.

Os requisitos da política de senha dependem do tipo de diretório que sua WorkMail organização Amazon usa.

Política de senha WorkMail do diretório Amazon e do Simple AD Directory

Por padrão, as senhas de um WorkMail diretório da Amazon ou do Simple AD devem ser:

- Não estarem vazias
- Ter pelo menos oito caracteres
- Ter menos de 64 caracteres
- Ser compostas por caracteres complementares do Latim básico ou Latim-1

As senhas também devem conter caracteres de três dos cinco dos seguintes grupos:

- Caracteres maiúsculos
- Caracteres minúsculos
- Ter dígitos numéricos (0 a 9)
- Caracteres especiais (por exemplo <, ~, ou !)
- Caracteres complementares do latim-1 (por exemplo é, ü, ou ñ)

As políticas de senha do WorkMail diretório Amazon não podem ser alteradas.

Para alterar uma política de senha do Simple AD, use as ferramentas de administração do AD em uma instância Windows do Amazon Elastic Compute Cloud (Amazon EC2) do seu diretório do Simple AD. Para obter mais informações, consulte Instalar as ferramentas de administração do Active Directory no Guia do administrador do AWS Directory Service.

Política de senhas do diretório do AWS Managed Microsoft AD

Para obter informações sobre a política de senha padrão para um diretório do AWS Managed Microsoft AD, consulte Gerenciar políticas de senha do AWS Managed Microsoft AD no Guia do administrador do AWS Directory Service.

Política de senha do AD Connector

O AD Connector usa a política de senha do domínio do Active Directory ao qual está conectado. Consulte a documentação do seu domínio do Active Directory para obter mais informações sobre as configurações da política de senha.

Trabalhar com notificações

Com a API de notificações WorkMail push da Amazon, você pode receber notificações push sobre alterações em sua caixa de correio, incluindo novas atualizações de e-mail e calendário. Você deve registrar as URLs (ou respondentes de notificação por push) para receber notificações. Com esse recurso, os desenvolvedores podem criar aplicativos responsivos para WorkMail usuários da Amazon, pois os aplicativos são rapidamente notificados sobre alterações na caixa de correio do usuário.

Para obter mais informações, consulte Assinaturas de notificações, eventos de caixa postal e EWS no Exchange.

Você pode assinar pastas específicas, como Caixa de entrada ou Calendário, ou todas as pastas para eventos de alteração de caixa de correio (incluindo e-mails novos, criados e modificados).

É possível usar bibliotecas clientes, como API Java do EWS ou a API gerenciado do EWS C# para acessar esse atributo. Uma amostra completa de um aplicativo de resposta push, desenvolvida usando o AWS Lambda e o API Gateway (usando a estrutura AWS Serverless), está disponível na página. AWS GitHub O aplicativo usa a API Java EWS.

Veja a seguir um exemplo de solicitação de assinatura via push:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://
schemas.microsoft.com/exchange/services/2006/types">
   <soap:Body>
      <m:Subscribe xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages">
         <m:PushSubscriptionRequest>
            <t:FolderIds>
               <t:DistinguishedFolderId Id="inbox" />
            </t:FolderIds>
            <t:EventTypes>
               <t:EventType>NewMailEvent</t:EventType>
               <t:EventType>CopiedEvent</t:EventType>
               <t:EventType>CreatedEvent</t:EventType>
               <t:EventType>DeletedEvent</t:EventType>
               <t:EventType>ModifiedEvent</t:EventType>
               <t:EventType>MovedEvent</t:EventType>
            </t:EventTypes>
            <t:StatusFrequency>1</t:StatusFrequency>
            <t:URL>https://YOUR_PUSH_RESPONDER_URL</t:URL>
         </m:PushSubscriptionRequest>
      </m:Subscribe>
   </soap:Body>
</soap:Envelope>
```

Veja a seguir um resultado bem-sucedido de solicitação de assinatura:

```
<?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>
```

Posteriormente, as notificações são enviadas para o URL especificado na solicitação de assinatura. Veja a seguir um exemplo de notificação:

```
<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>ygwAAAAAAA=</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 o respondente de notificações via push recebeu a notificação, ele deve responder com o seguinte:

```
<?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 o recebimento de notificações via push, os clientes devem enviar uma resposta de cancelamento de inscrição no campo `SubscriptionStatus`, parecido ao seguinte:

```
<?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 verificar a integridade do seu respondente de notificação push, a Amazon WorkMail envia um “heartbeat” (também chamado de`StatusEvent`). A frequência com que são enviadas é determinada pelo parâmetro `StatusFrequency` fornecido na solicitação de assinatura inicial. Por exemplo, se `StatusFrequency` for igual a **1**, é enviado um `StatusEvent` a cada 1 minuto. Esse valor pode estar em um intervalo entre 1 e 1440 minutos. Este `StatusEvent` se parece ao seguinte:

```
<?xml version="1.0 (http://www.w3.org/TR/REC-xml/)" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
    <t:RequestServerVersion xmlns:t="http://schemas.microsoft.com/exchange/
services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages" Version="Exchange2010_SP2"/>
</soap:Header>
<soap:Body>
    <m:SendNotification xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
    <m:ResponseMessages>
        <m:SendNotificationResponseMessage ResponseClass="Success">
            <m:ResponseCode>NoError</m:ResponseCode>
            <m:Notification>
                <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</t:SubscriptionId>
                <t:PreviousWatermark>AAAAAAAAAAA=</t:PreviousWatermark>
                <t:MoreEvents>false</t:MoreEvents>
                <t:StatusEvent>
                    <t:Watermark>AAAAAAAAAAA=</t:Watermark>
                </t:StatusEvent>
            </m:Notification>
        </m:SendNotificationResponseMessage>
    </m:ResponseMessages>
</m:SendNotification>
</soap:Body>
</soap:Envelope>
```

Se um cliente respondente de notificação por push não responder com o mesmo status anterior de 0K, a notificação será repetida por até `StatusFrequency` minutos. Por exemplo, se `StatusFrequency` for igual a 5, e a primeira notificação falhar, ela será repetida por, no máximo, 5 minutos com um recuo exponencial entre cada nova tentativa. Se a notificação não for entregue depois que o tempo de nova tentativa expirar, a assinatura será invalidada e não serão entregues novas notificações. Para continuar a receber notificações sobre eventos de caixa de correio, você deve criar uma nova assinatura. Atualmente, você pode se inscrever para, no máximo, três assinaturas por caixa postal.

Habilitar e-mails assinados ou criptografados

É possível usar S/MIME para permitir que usuários enviem e-mails assinados ou criptografados dentro e fora da organização.

> **Note**
>
> Os certificados de usuário da lista global de endereços (GAL) têm suporte apenas em uma configuração conectada do Active Directory.

Para permitir que os usuários enviem e-mails assinados ou criptografados

1. Configure um Active Directory (AD) Connector. A configuração de um AD Connector com o diretório local permite que os usuários continuem usando as credenciais corporativas existentes.
2. Configure a inscrição de certificados para emitir e armazenar certificados de usuários automaticamente no Active Directory. A Amazon WorkMail recebe certificados de usuário do Active Directory e os publica na GAL. Para obter mais informações, consulte Configure Certificate Autoenrollment.
3. Distribua os certificados gerados para os usuários exportando-os do servidor executando o Microsoft Exchange e enviando-os por e-mail.
4. Os usuários instalam o certificado no programa de e-mail (como o Windows Outlook) e nos dispositivos móveis.

Trabalhar com grupos de

Você pode usar grupos como listas de distribuição na Amazon WorkMail para receber e-mails de endereços de e-mail genéricos, como `<sales@example.com>` ou `<support@example.com>`. Você pode criar vários aliases de e-mail para um grupo.

Também é possível usar grupos como grupos de segurança para compartilhar uma caixa postal ou um calendário com uma equipe.

Os grupos não têm suas próprias caixas de correio, e isso afeta as permissões de caixa de correio que você pode conceder a um grupo. Para obter mais informações sobre como configurar permissões de caixa de correio para um grupo, consulte Gerenciar permissões de caixa de correio para grupos.

> **Note**
>
> Pode levar até duas horas para que os grupos recém-adicionados sejam exibidos no catálogo de endereços offline do Microsoft Outlook.

Tópicos

Visualizando uma lista de grupos

Para ver a lista de grupos

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da sua organização.
3. No painel de navegação, escolha Groups.
4. Além disso, você pode filtrar grupos por nome do grupo ou endereço de e-mail principal.

> **Note**
>
> A pesquisa diferencia maiúsculas de minúsculas.

Adicionar um grupo

Você pode adicionar grupos a partir do WorkMail console da Amazon.

Para adicionar um grupo

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Grupos e, em seguida, escolha Adicionar grupo.

   A página Adicionar grupo é exibida.
4. Em Nome do grupo, insira um nome para o grupo.
5. Em Endereço de e-mail, insira o endereço de e-mail principal do grupo.

6. Verifique o endereço de e-mail do grupo e atualize conforme necessário.
7. Por padrão, o grupo é exibido na lista de endereços global. Para ocultar o grupo da lista de endereços global, desmarque a caixa de seleção Mostrar na lista de endereços global.
8. Escolha Add Group (Adicionar grupo).

Habilitando grupos

Quando você integra a Amazon WorkMail com seu Active Directory corporativo, ou você já tem grupos disponíveis em seu Active Directory simples, você pode usar esses grupos como grupos de segurança ou listas de distribuição na Amazon WorkMail.

Para habilitar um grupo do diretório existente

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Groups.
4. Marque a caixa de seleção ao lado do grupo que você deseja habilitar e, em seguida, escolha Habilitar.

   A caixa de diálogo Habilitar grupos é exibida e solicita que você confirme a operação.
5. Conforme necessário, revise e altere o endereço de e-mail principal de cada grupo e escolha Habilitar.

Adicionar membros a um grupo

Depois de criar e habilitar um WorkMail grupo da Amazon, use o WorkMail console da Amazon para adicionar membros a esse grupo.

> **Note**
>
> Se a Amazon WorkMail estiver integrada a um serviço conectado do Active Directory ou ao Microsoft Active Directory, você poderá usar o Active Directory para gerenciar os membros do seu grupo. No entanto, as mudanças podem levar mais tempo para se propagar na Amazon WorkMail.

Para adicionar membros a um grupo

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e escolha o nome da organização.
3. No painel de navegação, escolha Groups.
4. Selecione o nome do grupo.
5. Na página de detalhes do grupo, escolha a guia Membros.
6. Escolha um grupo ou usuário para adicionar em Grupo ou Usuário.
7. Selecione o usuário ou grupo no menu suspenso.
8. Escolha Salvar.

As alterações podem levar alguns minutos para serem propagadas.

Editando detalhes do grupo

Você pode editar os detalhes de um grupo.

Para editar detalhes do grupo

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Grupos e selecione o grupo a ser editado.
4. Na página de detalhes do grupo, atualize o endereço de e-mail conforme necessário.
5. Por padrão, os grupos são exibidos na lista de endereços global. Para ocultar o grupo da lista de endereços global, desmarque a caixa de seleção Mostrar na lista de endereços global.
6. Escolha Salvar alterações.

Removendo membros de um grupo

Use o WorkMail console da Amazon para remover membros de um grupo.

> **Note**
>
> Se a Amazon WorkMail estiver integrada a um Active Directory ou Microsoft Active Directory conectado, você poderá usar o Active Directory para gerenciar os membros do seu grupo. No entanto, isso pode criar o tempo necessário para propagar suas alterações na Amazon WorkMail.

Para remover membros de um grupo

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e escolha o nome da organização.
3. No painel de navegação, selecione Grupos e, em seguida, escolha o nome do grupo.
4. Na página de detalhes do grupo, escolha a guia Membros.
5. Selecione o membro a ser removido do grupo.
6. Escolha Remover.

As alterações podem levar alguns minutos para serem propagadas.

Gerenciando aliases de grupos

Você pode adicionar ou remover aliases de e-mail dos grupos.

Para adicionar um alias de e-mail a um grupo.

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da organização para a qual você deseja adicionar um alias.
3. No painel de navegação, escolha Grupos e selecione o nome do grupo ao qual você deseja adicionar um alias.
4. Na seção Detalhes do grupo, escolha Aliases.
5. Em Aliases, escolha Adicionar alias.
6. Na caixa Alias, insira um alias.
7. Selecione um domínio para um alias.
8. Escolha Adicionar.

Para remover um alias de e-mail de um grupo.

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da organização da qual você deseja remover um alias.
3. No painel de navegação, escolha Grupos e, em seguida, selecione o nome do grupo do qual você deseja remover aliases.
4. Na seção Detalhes do grupo, escolha Aliases.
5. Em Aliases, marque a caixa de seleção dos aliases que você deseja remover.
6. Escolha Remover.

7. Verifique os aliases que serão removidos.
8. Na janela Remover aliases, escolha Remover.

Desativando grupos

Se você não precisar mais de um grupo, é possível desabilitá-lo.

Para desabilitar um grupo

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e escolha o nome da organização.
3. No painel de navegação, escolha Groups.
4. Em Nome do grupo, selecione os grupos a serem desativados e escolha Desativar.
5. Na caixa de diálogo Disable group(s), escolha Disable.

Excluir um grupo

Antes de excluir um grupo, você precisa primeiro desabilitá-lo. Para obter mais informações sobre como desabilitar grupos, consulte Desativando grupos.

Para excluir um grupo

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e escolha o nome da organização.
3. No painel de navegação, escolha Groups.
4. Marque a caixa de seleção ao lado do grupo desativado que você deseja excluir e escolha Excluir.

A caixa de diálogo Excluir é exibida.

5. Na caixa Digite o nome do grupo para confirmar a exclusão, insira o nome do grupo e escolha Excluir.

> **Note**
>
> Para excluir permanentemente um grupo, use a ação de `DeleteGroup` API para a Amazon WorkMail. Para obter mais informações, consulte DeleteGroupa Amazon WorkMail API Reference.

Trabalhar com recursos da

A Amazon WorkMail pode ajudar seus usuários a reservar recursos. Por exemplo, os usuários podem reservar salas de reunião ou equipamentos como projetores, telefones ou carros. Para reservar um recurso, o usuário o adiciona ao convite da reunião.

Tópicos

Visualizando uma lista de recursos

Para ver a lista de recursos

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da sua organização.
3. No painel de navegação, escolha Resources (Recursos).
4. Além disso, você pode filtrar recursos por nome do recurso ou endereço de e-mail principal.

> **Note**
>
> A pesquisa diferencia maiúsculas de minúsculas.

Adicionando um recurso

É possível adicionar um novo recurso à sua organização e permitir que ele seja reservado pelos usuários.

Para adicionar um recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Recursos e, em seguida, Adicionar recurso.

   A página Adicionar recurso é exibida.
4. Na caixa Nome do recurso, insira um nome para o recurso.
5. Como alternativa, na caixa Descrição do recurso, insira uma descrição para o recurso.
6. Em Tipo de recurso, escolha uma opção.
7. Verifique o endereço de e-mail do recurso e atualize conforme necessário.
8. Por padrão, o recurso é exibido na lista de endereços global. Para ocultar o recurso da lista de endereços global, desmarque a caixa de seleção Mostrar na lista de endereços global.
9. Selecione Adicionar recurso.

Editar detalhes do recurso

Você pode editar os detalhes gerais de um recurso, incluindo nome, descrição, tipo e endereço de e-mail, opções de reserva e representantes.

Para editar os detalhes gerais de um recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Resources e selecione o recurso a ser editado.
4. Na página Detalhes do recurso, atualize o nome do recurso, a descrição, o tipo de recurso ou o endereço de e-mail conforme necessário.
5. Por padrão, os recursos são exibidos na lista de endereços global. Para ocultar o recurso da lista de endereços global, desmarque a caixa de seleção Mostrar na lista de endereços global.
6. Escolha Salvar alterações.

É possível configurar um recurso para aceitar ou recusar reservas automaticamente.

Você pode editar as opções de reserva do recurso.

Para alterar as opções de reserva de um recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Resources e selecione o recurso a ser editado. Uma página é exibida e exibe os detalhes do recurso.
4. Em Opções de reserva, escolha Editar.
5. Conforme necessário, marque ou desmarque a caixa de seleção ao lado de uma opção para ativar ou desativar a opção.

> **Note**
>
> Ao desabilitar qualquer uma das opções de reserva automática, você deve criar um delegado para lidar com as solicitações de reserva. As próximas etapas explicam como criar um delegado.

Você pode adicionar um delegado para controlar as solicitações de reserva para um recurso que não tenha opções de reserva automática configuradas. Os representantes de recursos recebem automaticamente cópias de todas as solicitações de reserva e têm acesso total ao calendário de recursos. Além disso, eles devem aceitar todas as solicitações de reserva de um recurso.

Para adicionar um representante de recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, selecione Recursos e, em seguida, escolha o nome do recurso para o qual você quer adicionar um delegado.
4. (Opcional) Na guia Opções de reserva, escolha Editar, desmarque a caixa de seleção Aceitar automaticamente todas as solicitações de recursos e escolha Salvar.
5. Selecione a guia Delegados e, em seguida, escolha Adicionar delegado.

   A caixa de diálogo Adicionar delegado será exibida.
6. Abra a lista Pesquisar delegados, escolha um delegado e, em seguida, escolha Salvar.

Para remover um delegado de recursos

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da organização da qual você deseja remover os delegados.
3. No painel de navegação, escolha Recursos e selecione o nome do recurso do qual você deseja remover um representante.
4. Escolha Delegados e, em seguida, escolha o representante a ser removido.
5. Escolha Remover.

Gerenciando aliases de recursos

Você pode adicionar ou remover aliases de e-mail dos recursos.

Para adicionar um alias de e-mail a um recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da organização à qual você deseja adicionar um alias.
3. No painel de navegação, escolha Recursos e selecione o nome do recurso ao qual você deseja adicionar um alias.
4. Na seção Detalhes do recurso, escolha Aliases.
5. Em Aliases, escolha Adicionar alias.
6. Na caixa Alias, insira um alias.
7. Selecione um domínio para um alias.
8. Escolha Adicionar.

Para remover um alias de e-mail de um recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.

2. No painel de navegação, escolha Organizations e, em seguida, escolha o nome da organização da qual você deseja remover aliases.
3. No painel de navegação, escolha Recursos e, em seguida, selecione o nome do recurso do qual você deseja remover aliases.
4. Na seção Detalhes do recurso, escolha Aliases.
5. Em Aliases, marque a caixa de seleção dos aliases que você deseja remover.
6. Escolha Remover.
7. Verifique os aliases que serão removidos.
8. Na janela Remover aliases, escolha Remover.

Habilitar um recurso

Por padrão, a Amazon WorkMail cria um recurso. Se você ou outra pessoa desabilitar um recurso, você poderá reativá-lo em 30 dias.

Para habilitar um recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações sobre as regiões, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha a organização que contém o recurso que você deseja habilitar.
3. No painel de navegação, escolha Resources (Recursos).
4. Na lista de recursos, selecione o botão próximo ao recurso que você deseja habilitar e escolha Habilitar.

   A caixa de diálogo Habilitar recurso será exibida.
5. Escolha Habilitar.

Desabilitar um recurso

Quando você desabilita um recurso, você o torna indisponível para reserva. Por exemplo, você pode desabilitar uma sala de conferência enquanto ela está sendo reformada e, em seguida, habilitar a sala quando ela estiver disponível para uso.

Para desabilitar um recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações sobre as regiões, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha a organização que contém o recurso que você deseja desabilitar.
3. No painel de navegação, escolha Resources (Recursos).
4. Na lista de recursos, selecione o botão próximo ao recurso que você deseja desabilitar e escolha Desabilitar.

   A caixa de diálogo Desabilitar recurso será exibida.
5. Escolha Disable.

Excluir um recurso

Quando você não precisar mais de um recurso, poderá excluí-lo. No entanto, você deve primeiro desabilitar o recurso. Para obter informações sobre como desabilitar um recurso, consulte as etapas na seção anterior.

Para remover um recurso

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações sobre as regiões, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha a organização desejada.

3. No painel de navegação, escolha Resources (Recursos).
4. Na lista de recursos, selecione o botão próximo ao recurso desabilitado que você deseja remover e escolha Excluir.

   A caixa de diálogo Excluir recurso será exibida.
5. Na caixa Insira o nome do recurso para confirmar a exclusão, insira o nome do recurso que você deseja excluir e escolha Excluir recurso.

Trabalhar com dispositivos móveis

Os tópicos desta seção explicam como gerenciar dispositivos móveis conectados à Amazon WorkMail.

Tópicos

Editar a política de dispositivos móveis da sua organização

Você pode editar a política de dispositivos móveis da sua organização para mudar a forma como os dispositivos móveis interagem com a Amazon WorkMail.

Para editar a política de dispositivos móveis de uma organização

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a Região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Nome de regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Mobile Policies (Políticas de dispositivos móveis) e, na tela Mobile policy (Política de dispositivos móveis), escolha Edit (Editar).
4. Atualize as seguintes opções conforme necessário:

   a. Require encryption on device: criptografe os dados dos e-mails em dispositivos móveis.
   b. Require encryption on storage card: criptografe os dados dos e-mails no armazenamento removível de dispositivos móveis.
   c. Senha necessária: é necessária uma senha para bloquear um dispositivo móvel.
   d. Permitir senha simples: usar o PIN do dispositivo como senha.

e. Tamanho mínimo da senha: definir o número de caracteres necessários em uma senha válida.

f. Senha alfanumérica necessária: são necessárias senhas compostas por letras e números.

g. Número de tentativas malsucedidas: especifique o número de tentativas malsucedidas de desbloqueio do dispositivo que são permitidas antes que o dispositivo do usuário seja apagado. Todos os dados, incluindo arquivos pessoais, serão excluídos quando o dispositivo for apagado.

h. Password expiration: especifique o número de dias antes de uma senha vencer e precisar ser alterada.

i. Enable screen lock: especifique o número de segundos que leva para bloquear a tela de usuário quando ela ficar inativa.

j. Enforce password history: especifique o número de senhas que podem ser inseridas antes de repetir a mesma senha.

5. Selecione Salvar.

Gerenciar dispositivos móveis

Os tópicos desta seção explicam como apagar remotamente dispositivos móveis, remover dispositivos da sua organização e visualizar os detalhes dos dispositivos. Para obter informações sobre como editar a política de dispositivos móveis de sua organização, consulte Editar a política de dispositivos móveis da sua organização.

Tópicos

Apagar dispositivos móveis remotamente

As etapas desta seção explicam como apagar dispositivos móveis remotamente. Lembre-se do seguinte:

- Os dispositivos devem estar on-line e conectados à Amazon WorkMail. Se alguém desconectar o dispositivo, a operação de limpeza será retomada quando o usuário reconectar o dispositivo.

- As operações de limpeza podem levar cinco minutos para ser propagadas.

> **Important**
>
> Na maioria dos dispositivos móveis, a limpeza remota redefine o dispositivo aos padrões de fábrica. Todos os dados, inclusive arquivos pessoais, podem ser removidos ao realizar esse procedimento.

Para limpar remotamente o dispositivo móvel de um usuário

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a Região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Nome de regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, escolha Usuários, e na lista de usuários, selecione o nome do usuário cujo dispositivo você precisa apagar.
4. Escolha a guia Dispositivos móveis.
5. Na lista de dispositivos, selecione o botão próximo ao dispositivo e selecione Apagar.
6. Verifique o status na visão geral para ver se a limpeza foi solicitada.
7. Após o dispositivo ser apagado, é possível removê-lo da lista. As etapas da próxima seção explicam como fazer isso.

   > **Important**
   >
   > Para retornar um dispositivo apagado à lista de dispositivos de um usuário, primeiro remova-o da lista de dispositivos. Caso contrário, o sistema apaga o dispositivo novamente.

Remover dispositivos de usuários da lista de dispositivos

Se alguém parar de usar um dispositivo móvel específico ou se você tiver apagado o dispositivo remotamente, você poderá remover o dispositivo da lista de dispositivos. Quando o usuário configurar o dispositivo novamente, ele será exibido na lista.

Para remover dispositivos móveis de um usuário da lista de dispositivos

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a Região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. No painel de navegação, selecione Usuários e escolha o nome do usuário.
4. Escolha a guia Dispositivos móveis.
5. Na lista de dispositivos, selecione o botão próximo ao dispositivo e escolha Remover.

Visualizar detalhes de dispositivos móveis

É possível visualizar os detalhes do dispositivo móvel de um usuário.

> **Note**
>
> Alguns dispositivos não enviam todos os detalhes para o servidor. Talvez você não visualize todos os detalhes disponíveis do dispositivo.

Para ver detalhes do dispositivo

1. Abra o WorkMail console da Amazon em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da . Na barra de navegação, selecione a região que atende às suas necessidades. Para obter mais informações, consulte Regiões e endpoints na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.

3. No painel de navegação, selecione Usuários e escolha a guia Dispositivos móveis.
4. Na lista de dispositivos, selecione a ID do dispositivo cujos detalhes você quer visualizar.

   Os códigos de status do dispositivo estão indicados na tabela a seguir.

Status	Descrição
`PROVISIONING_REQUIRED`	Um usuário ou administrador solicitou que o dispositivo fosse provisionado para uso com a Amazon. WorkMail Os dispositivos também são configurados com esse status se a política atual desse dispositivo for modificada no WorkMail console da Amazon.
`PROVISIONING_SUCCEEDED`	O dispositivo foi provisionado com sucesso. O dispositivo aplicou a política fornecida.
`WIPE_REQUIRED`	Um administrador solicitou uma limpeza no WorkMail console da Amazon.
`WIPE_SUCCEEDED`	O dispositivo foi apagado.

Gerenciar regras de acesso a dispositivos móveis

As regras de acesso a dispositivos móveis do Amazon WorkMail permitem que os administradores controlem o acesso à caixa de correio para determinados tipos de dispositivos móveis. Por padrão, cada organização do Amazon WorkMail usa uma regra que concede acesso à caixa de correio a qualquer dispositivo, independentemente do tipo, modelo, sistema operacional ou atendente do usuário. Você pode editar ou substituir essa regra padrão por uma de sua preferência. Você também pode adicionar, alterar e excluir regras.

> **Warning**
>
> Se você excluir todas as regras de acesso a dispositivos móveis de uma organização, o Amazon WorkMail bloqueará todo o acesso a dispositivos móveis.

Você pode criar regras que permitam ou neguem o acesso com base nas seguintes propriedades do dispositivo:

- Tipo de dispositivo – "iPhone", "iPad" ou "Android".
- Modelo do dispositivo – "iPhone 10C1", "iPad 5C1" ou "HTC Onex".
- Sistema operacional do dispositivo — "iOS 12.3.1 16F203" ou "Android 8.1.0".
- Atendente de usuário do dispositivo — "iOS/14.2 (18B92) exchangesyncd/1.0" ou "Android-Mail/7.7.16.163886392.release".

Para visualizar as propriedades do dispositivo no AWS Management Console, consulte Visualização de detalhes do dispositivo móvel.

> **Note**
>
> Alguns dispositivos e clientes podem não relatar propriedades para todos os campos. Para obter informações sobre como contornar esses casos, consulte Dealing with empty fields

> **Important**
>
> As regras de acesso a dispositivos móveis do Amazon WorkMail se aplicam somente a dispositivos que usam o protocolo Microsoft Exchange ActiveSync. Clientes móveis que usam um protocolo diferente, como IMAP, não relatam as propriedades do dispositivo listadas aqui, portanto, essas regras não se aplicam.
> Se precisar restringir o acesso de dispositivos que usam outros protocolos, você pode criar regras de controle de acesso. Para obter mais informações, consulte Trabalhar com regras de controle de acesso . Como exemplo, você pode restringir o acesso a outros protocolos e webmail a apenas um intervalo de endereços IP corporativos, mas permitir o Microsoft ActiveSync de outro lugar e, em seguida, usar as regras de acesso a dispositivos móveis para limitar ainda mais os tipos e versões dos clientes permitidos.

Tópicos

Como funcionam as regras de acesso a dispositivos móveis

As regras de acesso a dispositivos móveis do Amazon WorkMail se aplicam somente a dispositivos que usam o protocolo Microsoft Exchange ActiveSync. Cada regra tem um conjunto de condições que especificam quando a regra se aplica, além de um efeito de acesso de `ALLOW` ou `DENY` para o dispositivo. Uma regra se aplica a uma solicitação de acesso somente se todas as condições da regra corresponderem às propriedades do dispositivo móvel do usuário. Regras sem condições se aplicam a todas as solicitações. Cada condição usa uma correspondência de prefixo que não diferencia maiúsculas de minúsculas com as propriedades relatadas do dispositivo.

O Amazon WorkMail avalia as regras da seguinte forma:

- Se alguma regra de `DENY` corresponder a uma propriedade do dispositivo, a política bloqueará o dispositivo. As regras de `DENY` têm precedência sobre as regras de `ALLOW`.
- Se pelo menos uma regra de `ALLOW` corresponder e nenhuma regra de `DENY` corresponder, a política permitirá o dispositivo.
- Se nenhuma regra se aplicar, o dispositivo será bloqueado.

> **Important**
>
> Os dispositivos móveis relatam as propriedades que as regras usam para funcionar. Os dispositivos relatam suas propriedades durante o processo de provisionamento do dispositivo do Microsoft ActiveSync. O Amazon WorkMail não pode verificar de forma independente se os clientes móveis relatam informações corretas ou atualizadas.

Usar regras de acesso a dispositivos móveis

Você pode usar APIs ou a AWS Command Line Interface (CLI) para criar e gerenciar regras de acesso a dispositivos móveis. Para mais informações sobre a AWS CLI, consulte o Guia do usuário da AWS Command Line Interface.

> **Important**
>
> Quando você altera uma regra de acesso para uma organização do Amazon WorkMail, os dispositivos afetados podem levar cinco minutos para seguir a regra atualizada, e os dispositivos podem mostrar um comportamento inconsistente durante esse período. No

entanto, você percebe imediatamente o comportamento correto ao testar as regras. Para obter mais informações, consulte Testing mobile device access rules.

Listar regras de acesso a dispositivos móveis

O exemplo a seguir mostra como listar as regras de acesso a dispositivos móveis.

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Criar regras de acesso a dispositivos móveis

O exemplo a seguir cria uma regra que bloqueia o acesso de todos os dispositivos Android às caixas de correio.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

O exemplo a seguir cria uma regra que permite somente uma versão específica do iOS. Certifique-se de remover a regra de `ALLOW-all` padrão.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

Atualizar regras de acesso a dispositivos móveis

O exemplo a seguir atualiza uma regra de dispositivo adicionando um 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"
```

Excluir uma regra de acesso a dispositivos móveis

O exemplo a seguir exclui a regra de acesso ao dispositivo móvel com o identificador fornecido.

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

Testar regras de acesso a dispositivos móveis

Para testar as regras de acesso, você pode usar a API GetMobileDeviceAccessEffect ou o comando get-mobile-device-access-effect na AWS CLI . Para obter mais informações sobre a AWS CLI, consulte o Guia do usuário da AWS Command Line Interface.

Ao testar, você passa as propriedades de um dispositivo móvel simulado, e a API ou a CLI retornam o efeito de acesso, `ALLOW` ou `DENY`, que um dispositivo móvel real com essas propriedades receberia. Por exemplo, esse comando testa se um iPhone executando o iOS 14.2, além do aplicativo de e-mail padrão, pode acessar uma caixa de correio.

```
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"
```

Lidar com campos vazios

Alguns dispositivos móveis ou clientes podem não relatar informações para um ou mais campos, deixando os valores vazios. As regras podem corresponder a esses dispositivos usando o valor especial `$NONE` em uma condição. Por exemplo, uma regra com `DeviceTypes=["iphone", "ipad", "$NONE"]` corresponderá a dispositivos que relatam um tipo de dispositivo `"iphone"` ou `"ipad"`, ou que não relatam nenhum tipo de dispositivo.

Condições negativas, como `NotDeviceTypes` ou `NotDeviceUserAgents` não corresponderão a esses valores vazios. Por exemplo, uma regra com `NotDeviceTypes=["android"]` corresponderá a dispositivos que relatam um tipo de dispositivo diferente de `"android"`. No entanto, a regra não corresponderá a dispositivos que não relatam nenhum tipo de dispositivo.

Gerenciar substituições de acesso a dispositivos móveis

Você usa substituições de acesso a dispositivos móveis para substituir os resultados das regras de acesso a dispositivos móveis. As substituições se aplicam a usuários e dispositivos específicos e revertem a regra de acesso padrão. Você também pode usar substituições para criar exceções únicas para acessar regras e permitir ou negar pares específicos de usuários e dispositivos. Além

disso, você pode usar substituições com uma regra de acesso `DefaultDenyAll` a dispositivos móveis. Isso adia as decisões de acesso para uma solução de gerenciamento de dispositivos móveis (MDM) de terceiros. Para obter mais informações, consulte Gerenciar substituições e Integração com soluções de gerenciamento de dispositivos móveis

Tópicos

Como gerenciar substituições de acesso a dispositivos móveis

As substituições de acesso a dispositivos móveis são criadas para um par específico de usuário e dispositivo. A substituição reverte o resultado de acesso padrão ao avaliar as regras de acesso de dispositivos móveis para um determinado usuário e dispositivo. Por exemplo, se uma regra de acesso normalmente nega o acesso, uma substituição de acesso permite que o usuário e o dispositivo sincronizem seus e-mails. Por outro lado, se uma regra de acesso normalmente permite o acesso, você pode criar uma substituição que impeça o usuário e o dispositivo de sincronizar seus e-mails. Quando você exclui uma substituição de acesso a um dispositivo móvel, a Amazon WorkMail novamente respeita o resultado das regras atuais de acesso a dispositivos móveis ao decidir se concede acesso a esse usuário e dispositivo.

> **Important**
>
> Quando você altera a substituição de um dispositivo móvel para uma WorkMail organização da Amazon, os dispositivos afetados podem levar cinco minutos para seguir a substituição atualizada.

Gerenciar substituições

As substituições de acesso a dispositivos móveis podem ser criadas, atualizadas ou excluídas usando a API ou AWS Command Line Interface. Para obter mais informações sobre o AWS CLI, consulte o Guia do usuário da interface de linha de comando da AWS.

Para encontrar o ID do dispositivo, use o AWS Management Console. Para obter mais informações, consulte Visualizar detalhes de dispositivos móveis.

Listar substituições de acesso a dispositivos móveis

Este exemplo mostra como listar todas as substituições de acesso a dispositivos móveis para uma organização específica da Amazon WorkMail .

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Criar e atualizar substituições de acesso a dispositivos móveis

Isso criará uma substituição de acesso ao dispositivo móvel para negar o acesso à WorkMail organização, ao usuário e ao ID do dispositivo especificados da Amazon.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect DENY
```

Uma substituição de acesso a um dispositivo móvel existente pode ser modificada para ter um efeito diferente. Isso atualizará a substituição de acesso ao dispositivo móvel criada anteriormente para permitir o acesso em vez de negar.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect ALLOW
```

Excluir substituições de acesso a dispositivos móveis

Isso excluirá a substituição do acesso ao dispositivo móvel para a WorkMail organização, o usuário e o ID do dispositivo especificados da Amazon.

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0
```

Integração com soluções de gerenciamento de dispositivos móveis

A Amazon WorkMail oferece suporte a alguns recursos básicos de gerenciamento de dispositivos móveis por meio de políticas de dispositivos móveis e regras de acesso a dispositivos móveis. No entanto, esses recursos só podem interagir com dispositivos móveis por meio do protocolo Microsoft Exchange ActiveSync (EAS), portanto, eles têm capacidade limitada de introspectar e impor a postura de segurança do dispositivo. Os administradores que precisam de maior controle sobre

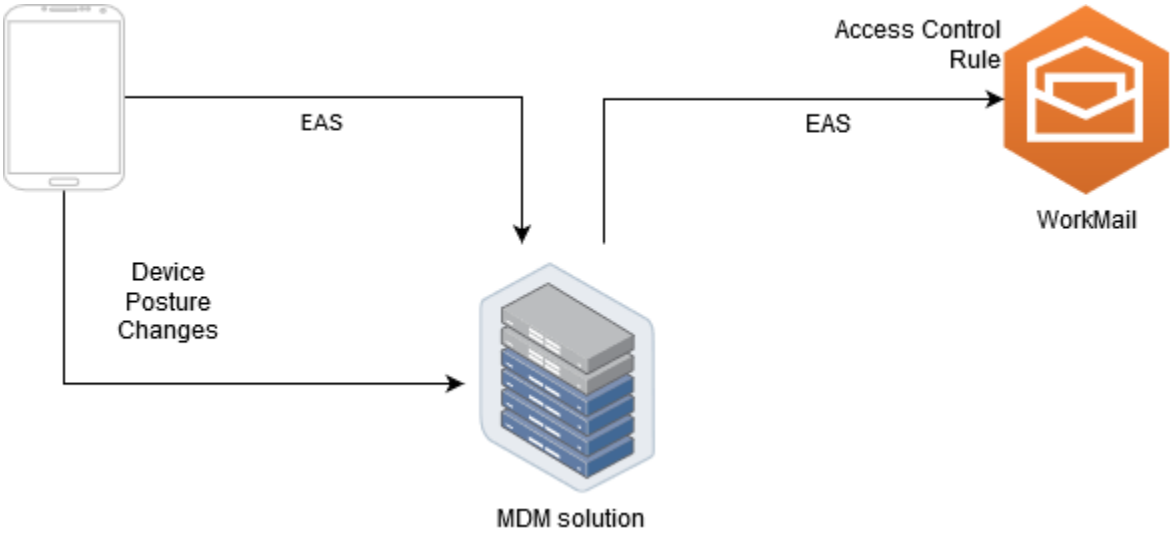
a segurança e a conformidade dos dispositivos podem usar uma solução de gerenciamento de dispositivos móveis (MDM) de terceiros.

Visão geral das soluções de gerenciamento de dispositivos móveis

Você pode configurar sua solução de MDM em dois modos, proxy ou direto. Consulte a documentação do MDM para ver quais modos sua solução suporta.

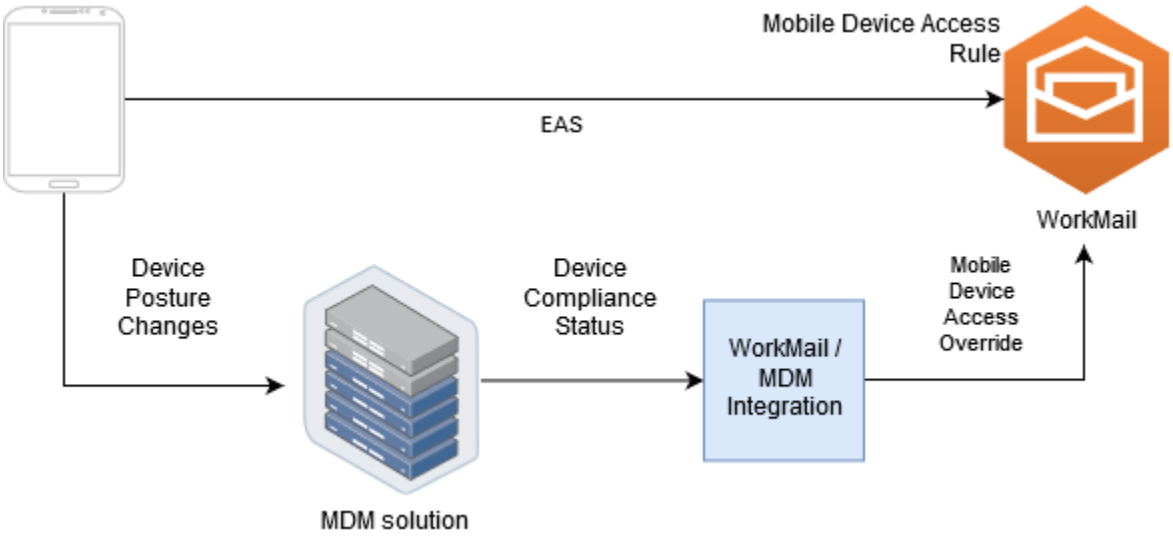
No modo proxy, os dispositivos móveis usam o protocolo Exchange Active Sync (EAS) por meio de sua solução MDM para acessar a Amazon WorkMail. A solução MDM usa a postura do dispositivo para permitir ou negar acesso aos dados da Amazon WorkMail. No WorkMail lado da Amazon, use uma regra de controle de acesso que permita o acesso ao EAS somente a partir do endereço ou endereços IP da solução MDM. Para obter mais informações, consulte Trabalhar com regras de controle de acesso.

A imagem a seguir mostra uma configuração típica do modo proxy.



No modo direto, os dispositivos móveis usam o EAS para acessar a Amazon WorkMail diretamente. Sua solução de MDM recebe mudanças na postura do dispositivo e avalia continuamente se cada dispositivo atende a esses requisitos. Quando a solução MDM detecta uma mudança de postura, como um dispositivo que está saindo de conformidade, ela pode realizar várias ações e normalmente emite notificações ou eventos. Um WorkMail administrador da Amazon pode configurar um sistema para ouvir esses eventos de status de conformidade e criar automaticamente substituições de acesso a dispositivos móveis que permitem ou negam acesso aos dispositivos quando eles entram ou não estão em conformidade com os requisitos do dispositivo MDM.

A imagem a seguir mostra uma configuração típica do modo direto.



Configurando uma WorkMail organização para se integrar a uma solução MDM de terceiros no modo direto

Para se integrar a uma solução de gerenciamento de dispositivos móveis (MDM) de terceiros no modo direto, você deve atender aos seguintes requisitos:

- Crie regras de controle de acesso que restrinjam o acesso aos dispositivos do usuário somente ao ActiveSync protocolo.
- Crie uma regra padrão de acesso a dispositivos móveis deny-to-all "" para garantir que todos os dispositivos móveis desconhecidos ou não gerenciados sejam negados por padrão.
- Adote uma solução de gerenciamento de dispositivos móveis que emita notificações ou eventos personalizados quando um dispositivo muda a postura de segurança, o que significa que ele entra ou sai de conformidade.
- Crie um componente de software personalizado para ouvir essas notificações e ligue para o Amazon WorkMail SDK para criar substituições de acesso a dispositivos móveis.

Esses componentes garantem que todos os dispositivos do usuário atendam aos requisitos de conformidade do MDM antes de serem autorizados a acessar suas caixas de WorkMail correio da Amazon.

Use regras de controle de acesso para restringir o acesso de dispositivos móveis a ActiveSync

Você deve garantir que todos os dispositivos usem somente o ActiveSync protocolo, e você pode usar as regras de controle de acesso para fazer isso. Por exemplo, você pode conceder acesso a

outros protocolos de e-mail somente a partir de um intervalo interno de endereços IP corporativos e, em seguida, permitir somente ActiveSync ao acessar e-mails de fora do firewall corporativo. Você deve fazer isso porque só ActiveSync permite identificar dispositivos usando uma ID de dispositivo. Você não pode usar protocolos como o Internet Message Access Protocol (IMAP) ou o Exchange Web Services. Para ter mais informações, consulte Trabalhar com regras de controle de acesso.

Criar uma regra de acesso padrão de "negar a todos"

Para transferir todas as decisões de acesso a dispositivos móveis para a solução de gerenciamento de dispositivos móveis de terceiros, crie uma regra de acesso que negue automaticamente todos os dispositivos, a menos que seja substituída para cada usuário ou dispositivo. Para mais informações, consulte Gerenciar regras de acesso a dispositivos móveis.

Este exemplo mostra uma regra de "negar a todos".

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

Reagir a mudanças de postura do dispositivo e criar substituições de acesso a dispositivos móveis

Você deve configurar sua solução de MDM para enviar notificações sobre alterações na postura do dispositivo. Essas notificações devem ser consumidas por um componente que pode usar o Amazon WorkMail SDK para criar ou atualizar substituições de acesso a dispositivos móveis. Por padrão, a Amazon WorkMail nega acesso a dispositivos não gerenciados ou recém-provisionados devido à regra padrão de “negar a todos” o acesso a dispositivos móveis mostrada anteriormente neste tópico. Quando a solução de MDM determina que o dispositivo atende a todos os requisitos e emite uma notificação indicando que o dispositivo está em conformidade, esse componente pode reagir a essa notificação criando uma substituição de acesso ao dispositivo móvel com um efeito de `ALLOW` para o usuário e o dispositivo específicos. Se o dispositivo sair de conformidade posteriormente, a solução de gerenciamento de dispositivos móveis emitirá outra notificação e a substituição do acesso poderá ser excluída ou modificada para negar o acesso a esse dispositivo. Para ter mais informações, consulte Gerenciar substituições de acesso a dispositivos móveis.

Para ver um exemplo da Amazon WorkMail integrada ao MDM, consulte este AWS exemplo de aplicativo.

Trabalhar com permissões de caixa de correio

Você pode usar permissões de caixa de correio no Amazon WorkMail para conceder aos usuários ou grupos o direito de trabalhar nas caixas de correio de outros usuários. As permissões de caixa de correio se aplicam a uma caixa de correio completa. Elas permitem que vários usuários acessem a mesma caixa de correio sem compartilhar as credenciais dessa caixa de correio. Os usuários com permissões de caixa de correio podem ler e modificar dados da caixa de correio, além de enviar e-mails da caixa de correio compartilhada.

> **Note**
>
> Usuários com permissões para uma caixa de correio pertencente a um usuário oculto na lista de endereços global ainda podem acessar a caixa de correio do usuário oculto.

A lista a seguir mostra as permissões que você pode conceder:

- Acesso total: permite acesso total de leitura e escrita à caixa de correio, incluindo permissões para modificar as permissões no nível da pasta.

  > **Note**
  >
  > Essas opções estão disponíveis somente para usuários. Não é possível conceder direitos de acesso total aos grupos.

- Enviar em nome de: permite que um usuário ou grupo envie e-mails em nome de outro usuário. O proprietário da caixa de correio aparece no cabeçalho De: e o remetente aparece no cabeçalho Remetente:.
- Enviar como: permite que um usuário ou grupo envie e-mails como o proprietário da caixa de correio, sem exibir o remetente real da mensagem. O proprietário da caixa de correio aparece nos cabeçalhos De: e Remetente:.
- Nenhum: impede que um usuário ou grupo envie e-mails.

> **Note**
>
> Conceder permissões de caixa de correio a um grupo estende essas permissões a todos os membros desse grupo, incluindo membros de grupos aninhados.

Ao conceder permissões de caixa de correio, o serviço AutoDiscover do Amazon WorkMail atualiza automaticamente o acesso a essas caixas de correio para os usuários ou grupos que você adicionou.

Para o cliente do Microsoft Outlook no Windows, os usuários com permissões de acesso total podem acessar automaticamente as caixas de correio compartilhadas. Aguarde até 60 minutos para que as alterações sejam propagadas e, em seguida, reinicie o Microsoft Outlook.

Para o aplicativo Web do Amazon WorkMail e outros clientes de e-mail, os usuários com permissões de acesso total podem abrir manualmente as caixas de correio compartilhadas. As caixas de correio abertas permanecem abertas, mesmo entre as sessões, a menos que o usuário as feche.

Tópicos

Sobre permissões de caixa de correio e de pasta

As permissões de caixa de correio se aplicam a todas as pastas em uma caixa de correio. Essas permissões só podem ser habilitadas pelo proprietário da conta da AWS ou um usuário do IAM autorizado a chamar a API de gerenciamento do Amazon WorkMail. Para definir e alterar permissões para caixas de correio ou para grupos como um todo, use a API do AWS Management Console ou do Amazon WorkMail. É possível gerenciar até 100 permissões a caixas correio e grupos no console. Para gerenciar permissões para mais usuários e grupos, use a API do Amazon WorkMail.

As permissões de pasta se aplicam somente a uma única pasta. Essas permissões podem ser definidas por usuários finais usando um cliente de e-mail ou o aplicativo web do Amazon WorkMail. Para obter mais informações sobre o uso do aplicativo web do Amazon WorkMail para compartilhar pastas, consulte Compartilhamento de pastas e permissões de pastas no Guia do usuário do Amazon WorkMail.

Gerenciar permissões de caixa de correio para usuários

Você pode usar o console do Amazon WorkMail para gerenciar permissões de caixa de correio para usuários e grupos. As seções a seguir descrevem como gerenciar permissões para usuários. Para obter mais informações sobre como gerenciar permissões para grupos, consulte Gerenciar permissões de caixa de correio para grupos.

Tópicos

Adicionar permissões

Ao adicionar permissões, você concede a um usuário o direito de realizar uma ou mais tarefas na caixa de correio de outro usuário. Por exemplo, digamos que o funcionário A precise enviar mensagens em nome do seu supervisor, o funcionário B. Para conceder essa permissão, acesse as configurações da caixa de correio do funcionário B e conceda ao funcionário A permissão para realizar a tarefa solicitada.

Para adicionar permissões de caixa de correio

1. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da . Na barra de navegação, escolha a região que atende às suas necessidades. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização à qual você deseja gerenciar permissões.
3. No painel de navegação, selecione Usuários e, em seguida, escolha o nome do usuário ao qual você deseja gerenciar permissões.
4. Selecione a guia Permissões e escolha Adicionar permissões.

   A caixa de diálogo Adicionar permissões será exibida.
5. Abra a lista Adicionar novas permissões e selecione o usuário ou grupo que precisa acessar a caixa de correio.
6. Em Permissões de caixa de correio e Permissões de envio, escolha as opções desejadas.

7. Escolha Add (Adicionar).

As novas permissões podem levar até cinco minutos para serem propagadas aos usuários.

Editar permissões de caixa de correio para usuários

Ao editar as permissões de caixa de correio para um usuário, você altera o acesso que outras pessoas têm à caixa de correio desse usuário. Editar as permissões de caixa de correio não altera o acesso do usuário original da caixa de correio.

Para editar permissões de caixa de correio

1. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da . Na barra de navegação, escolha a região que atende às suas necessidades. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização à qual você deseja gerenciar permissões.
3. No painel de navegação, selecione Usuários e, em seguida, o nome do usuário cujas permissões você deseja editar.
4. Escolha a aba Permissions (permissões).

   Uma lista dos usuários e grupos que têm acesso à caixa de correio será exibida.
5. Selecione o botão de opção ao lado do usuário ou grupo que você deseja alterar e, em seguida, siga umas das seguintes opções:

   Para remover as permissões de um usuário

   1. Escolha Remove.

      A caixa de diálogo Remover permissões será exibida.
   2. Na caixa de diálogo Remover permissões, selecione Remover.

   Para editar as permissões de um usuário

   1. Escolha Editar.

A caixa de diálogo Editar permissões será exibida.

2. Defina as permissões conforme necessário e, em seguida, selecione Salvar.

Para conceder a outro usuário permissões para a caixa de correio

1. Escolha Add permissions (Adicionar permissões).

   A caixa de diálogo Adicionar permissões será exibida.

2. Abra a lista Adicionar novas permissões e selecione o usuário que você deseja adicionar.
3. Defina as permissões conforme necessário e, em seguida, selecione Adicionar.

As novas permissões podem levar até cinco minutos para serem propagadas aos usuários.

Gerenciar permissões de caixa de correio para grupos

Você pode adicionar ou remover as permissões de grupo do Amazon WorkMail.

> **Note**
>
> Você não pode aplicar permissões de Acesso total a um grupo, porque os grupos não têm uma caixa de correio para acessar.

Para gerenciar permissões de grupo

1. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a Região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização à qual você deseja gerenciar permissões.
3. No painel de navegação, selecione Grupos e, em seguida, escolha o nome do grupo ao qual você deseja definir permissões.
4. Selecione a guia Permissões e escolha Adicionar permissões.

A caixa de diálogo Adicionar permissões será exibida.

5. Abra a lista Adicionar novas permissões e selecione o usuário ou grupo que receberá acesso à caixa de correio.
6. Em Permissões de caixa de correio e Permissões de envio, escolha as opções desejadas.
7. Escolha Add (Adicionar).

As novas permissões podem levar até cinco minutos para serem propagadas aos usuários.

Acesso programático às caixas de correio

Para acessar programaticamente as caixas de correio do Amazon WorkMail, use o protocolo Exchange Web Services (EWS). Com o EWS, você pode acessar todos os tipos de itens em uma caixa de correio. Aqui estão algumas bibliotecas do EWS que você pode usar com o Amazon WorkMail:

- Java – API Java do EWS
- .Net – API gerenciada do EWS
- Python – Exchangelib

O Amazon WorkMail também suporta protocolos IMAP e SMTP, que podem ser usados para enviar e receber e-mail. Você pode ver as URLs compatíveis com os protocolos do Amazon WorkMail em endpoints e cotas do Amazon WorkMail.

Ao usar o protocolo EWS, o Amazon WorkMail oferece suporte aos seguintes métodos de autenticação:

- Autenticação básica – Com a autenticação básica, você insere um endereço de e-mail e senha.
- Funções de personificação – Com as funções de personificação, você acessa as caixas de correio dos usuários sem inserir as credenciais do usuário.

Tópicos

Gerenciamento de funções de personificação

Com as funções de personificação, os administradores configuram o acesso programático às caixas de correio do usuário sem inserir as credenciais do usuário. Serviços e ferramentas podem assumir uma função de personificação para realizar ações nas caixas de correio do usuário. A personificação só é compatível com o protocolo EWS.

Visão geral das funções de personificação

Para permitir a personificação, os administradores devem criar uma função de personificação com as seguintes propriedades:

- Tipo de função – Escolha Acesso total ou Somente leitura. O tipo de função limita o tipo de operações que uma função pode realizar.
- Regras – Uma lista de regras que definem quais usuários a função de personificação pode representar.

O Amazon WorkMail avalia as regras nas seguintes condições:

- Se alguma regra DENY corresponder, a política nega a personificação. As regras DENY têm precedência sobre quaisquer regras ALLOW.
- Se pelo menos uma regra ALLOW corresponder e nenhuma regra DENY corresponder, a política permitirá a personificação.
- Se nenhuma regra se aplicar, a personificação será negada.

> **Note**
>
> Para permitir a personificação de todos os usuários em uma organização do Amazon WorkMail, crie uma regra com efeito ALLOW e sem condições.

> **Warning**
>
> Você deve criar regras para permitir que uma função de personificação se faça passar por um usuário. Se você não especificar regras, uma função de personificação não poderá assumir os direitos de acesso de um usuário.

Depois que a função de personificação for criada, você poderá usá-la para obter acesso às caixas de correio dos usuários. Para obter mais informações, consulte Usar funções de personificação.

Considerações sobre segurança

O uso de funções de personificação cria possíveis problemas de segurança em sua organização do Amazon WorkMail e Conta da AWS. Aqui estão alguns dos possíveis problemas a serem considerados ao criar uma função de personificação:

- Permissões transitivas – Se o usuário A tiver acesso à caixa de correio do usuário B e uma função de personificação tiver permissão para se passar pelo usuário A, essa função de personificação poderá imitar as permissões de acesso do usuário A e acessar a caixa de correio do usuário B.
- Controle de acesso – Você pode usar regras de controle de acesso para limitar o acesso da função de personificação. Para obter mais informações, consulte Trabalhar com regras de controle de acesso.
- Política do IAM – Você pode atribuir uma ação de `AssumeImpersonationRole` a uma organização específica do Amazon WorkMail e a uma função de personificação usando a condição `workmail:ImpersonationRoleId`. Para ver um exemplo de política do IAM, consulte Como a Amazon WorkMail trabalha com o IAM.

Criar funções de personificação

Você pode criar funções de personificação a partir do console do Amazon WorkMail.

Para criar uma função de personificação

1. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da . Na barra de navegação, escolha a região que atende às suas necessidades. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Funções de personificação e, em seguida, escolha Criar função.
4. A caixa de diálogo Criar função de personificação será exibida. Em Função, insira as informações a seguir:

   - Nome – Insira um nome exclusivo para a função de personificação.
   - (Opcional) Descrição – Insira uma descrição para a nova função de personificação.
   - Tipo de função – Escolha Somente leitura ou Acesso total.

5. Em Regras, escolha Adicionar regra.
6. A caixa de diálogo Adicionar regra será exibida. Insira as seguintes informações:
   - Nome – Insira um nome exclusivo para a regra.
   - (Opcional) Descrição – Insira uma descrição para a regra.
   - Em Efeito, escolha Permitir ou Negar. Isso permite ou nega o acesso com base nas condições selecionadas na etapa a seguir.
   - (Opcional) Em Esta regra:, escolha Corresponde às solicitações que se fazem passar pelos usuários selecionados para incluir usuários específicos. Escolha Corresponde a solicitações que se fazem passar por usuários diferentes dos selecionados para adicionar usuários que não sejam os selecionados.
7. Escolha Add rule (Adicionar regra).

> **Note**
>
> As regras só são salvas quando você salva a função correspondente.

8. Selecione Create role (Criar função).

Editar funções de personificação

Você pode editar funções de personificação a partir do console do Amazon WorkMail.

Para editar uma função de personificação

1. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da . Na barra de navegação, escolha a região que atende às suas necessidades. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Funções de personificação.
4. Selecione o nome da função de personificação que deseja editar e, em seguida, escolhaEditar.
5. A caixa de diálogo Editar função de personificação será exibida. Em Função, insira as informações a seguir:

- Nome – Insira um nome exclusivo para a função de personificação.
- (Opcional) Descrição – Insira uma descrição para a nova função de personificação.
- Tipo de função – Para conceder à função de personificação acesso somente para leitura à caixa de correio de um usuário, escolha Somente leitura. Para conceder à função de personificação direitos de ler e modificar itens na caixa de correio de um usuário, escolha Acesso total.

6. Em Regras, selecione a regra que você deseja editar e escolha Editar.
7. A caixa de diálogo Editar regra será exibida. Insira as seguintes informações:

   - Nome – Edite o nome da regra.
   - (Opcional) Descrição – Atualize ou insira uma descrição para a regra.
   - Em Efeito, escolha Permitir para permitir o acesso quando as condições definidas nas regras forem atendidas. Para negar acesso, escolha Negar.
   - (Opcional) Em Esta regra:, escolha Corresponde às solicitações que se fazem passar pelos usuários selecionados para incluir usuários específicos. Escolha Corresponde a solicitações que se fazem passar por usuários diferentes dos selecionados para adicionar usuários que não sejam os selecionados.
8. Escolha Save (Salvar).
9. Escolha Save changes (Salvar alterações).

> **Important**
>
> Quando você altera uma regra de personificação, as caixas de correio afetadas podem levar até cinco minutos para serem atualizadas. Durante o processo de atualização da regra, você pode observar um comportamento inconsistente na sua caixa de correio. No entanto, se você testar uma função, o Amazon WorkMail responderá conforme o esperado com base na regra atualizada. Para obter mais informações, consulte Testar funções de personificação.

Testar funções de personificação

Você pode testar funções de personificação a partir do console do Amazon WorkMail.

Para testar uma função de personificação

1. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da . Na barra de navegação, escolha a região que atende às suas necessidades. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Funções de personificação.
4. Selecione a função de personificação que deseja testar.
5. Escolha Testar função.
6. A caixa de diálogo Testar função de personificação será exibida. Em Usuário alvo, selecione o usuário para o qual você deseja testar o acesso de personificação.
7. Escolha Test (Testar).

Excluir funções de personificação

Você pode excluir funções de personificação a partir do console do Amazon WorkMail.

Para excluir uma função de personificação

1. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da . Na barra de navegação, escolha a região que atende às suas necessidades. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e, em seguida, escolha o nome da organização.
3. Escolha Funções de personificação.
4. Selecione o nome da função de personificação que deseja excluir.
5. Escolha Delete (Excluir).
6. A caixa de diálogo Excluir função será exibida. Para confirmar a exclusão, insira o nome da função na caixa de diálogo e escolha Excluir.

Usar funções de personificação

Para acessar os dados da caixa de correio, use a ação de API `AssumeImpersonationRole` do Amazon WorkMail. Para obter mais detalhes sobre as APIs do Amazon WorkMail, consulte Referência de API.

`AssumeImpersonationRole` retorna um `Token`. Esse `Token` deve ser passado em 15 minutos para o protocolo EWS por meio do cabeçalho HTTP `Authorization`.

Os exemplos a seguir demonstram como usar funções de personificação com o protocolo EWS. As constantes usadas nos exemplos especificam os seguintes detalhes exclusivos de sua organização e conta:

- *`WORKMAIL_ORGANIZATION_ID`* – ID da organização do Amazon WorkMail
- *`IMPERSONATION_ROLE_ID`* – ID da função de personificação
- *`WORKMAIL_EWS_URL`* – Endpoint EWS disponível em endpoints e cotas do Amazon WorkMail
- *`EMAIL_ADDRESS`* – Endereço de e-mail da caixa de correio do usuário

Example Java – API Java do 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 gerenciada do 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
)
```

Exportar conteúdo de caixa de correio

Use a ação de API StartMailboxExportJob na Referência de API do Amazon WorkMail para exportar conteúdo de caixa de correio do Amazon WorkMail para um bucket do Amazon Simple Storage Service (Amazon S3). Essa ação exporta todas as mensagens de e-mail e itens de calendário da caixa de correio especificada para um arquivo `.zip` no bucket do Amazon S3, no formato MIME. Outros itens, como contatos e tarefas, não são exportados.

O tempo necessário para a conclusão do trabalho de exportação da caixa de correio depende do tamanho e do número de itens na caixa de correio. Como o trabalho de exportação da caixa de correio ocorre durante um período de tempo, ele não representa um snapshot do conteúdo da caixa de correio em um único momento. Para ver o status de um trabalho de exportação, use as ações de API DescribeMailboxExportJob ou ListMailboxExportJobs na Referência de API do Amazon WorkMail.

Quando um trabalho de exportação de caixa de correio é concluído, o arquivo `.zip` no bucket do Amazon S3 é criptografado usando a chave mestra do cliente (CMK) AWS Key Management Service simétrica (AWS KMS) que você fornece. Como a criptografia AWS KMS é integrada ao Amazon S3, os dados descriptografados ficam visíveis para o usuário que os baixa, desde que o usuário tenha acesso à CMK AWS KMS.

Pré-requisitos

Estes são os pré-requisitos para exportar conteúdo de caixa de correio:

- A capacidade de programar.
- Uma conta de administrador do Amazon WorkMail.
- Um bucket do Amazon S3 que não permite acesso público. Para obter mais informações, consulte Como usar o Bloqueio de Acesso Público do Amazon S3 no Guia do usuário do Amazon Simple Storage Service e no Guia do usuário do Amazon Simple Storage Service.
- Uma CMK AWS KMS simétrica Para obter mais informações, consulte Conceitos básicos no Guia do desenvolvedor do AWS Key Management Service.
- Um perfil do AWS Identity and Access Management (IAM) com uma política que concede permissão para gravar no bucket do Amazon S3 e criptografar os arquivos enviados com a CMK AWS KMS. Para obter mais informações, consulte Como a Amazon WorkMail trabalha com o IAM.

Exemplos de política do IAM e criação de perfil

O exemplo a seguir mostra uma política do IAM que concede permissão para gravar no bucket do Amazon S3 e criptografar os arquivos enviados com a CMK AWS KMS. Para usar esse exemplo de política no procedimento Exemplo: exportar conteúdo da caixa de correio a seguir, salve a política como um arquivo JSON com nome de arquivo `mailbox-export-policy.json`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:GetBucketPolicyStatus"
            ],
            "Resource": [
                "arn:aws:s3:::AWSDOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::AWSDOC-EXAMPLE-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:::AWSDOC-EXAMPLE-
BUCKET/S3-PREFIX*"
                }
            }
        }
    ]
```

```
}
```

O exemplo a seguir mostra uma política confiável do IAM anexada ao perfil do IAM que você criou. Para usar esse exemplo de política no procedimento Exemplo: exportar conteúdo da caixa de correio a seguir, salve a política como um arquivo JSON com nome de arquivo `mailbox-export-trust-policy.json`.

Você não precisa usar as condições `aws:SourceArn` e `aws:SourceAccount` ao mesmo tempo. Por exemplo, você pode remover `aws:SourceArn` da política se precisar usar o mesmo perfil para exportar mensagens de diferentes organizações do Amazon WorkMail sob a mesma conta AWS. Para obter mais informações sobre chaves de condição, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do AWS Identity and Access Management.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmail:us-east-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
        }
      }
    }
  ]
}
```

Você pode usar a AWS CLI para criar o perfil do IAM em sua conta executando os comandos a seguir.

```
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 obter mais informações sobre a AWS CLI, consulte o AWS Command Line InterfaceManual do usuário da .

Exemplo: exportar conteúdo da caixa de correio

Depois de criar as políticas e o perfil do IAM na seção anterior, conclua as etapas a seguir para exportar o conteúdo da sua caixa de correio. Você precisa ter o ID da organização e o ID do usuário (ID da entidade) do Amazon WorkMail, que podem ser acessados no console do Amazon WorkMail ou usando a API do Amazon WorkMail.

Exemplo: exportar conteúdo da caixa de correio

1. Use a AWS CLI para iniciar o trabalho de exportação da caixa de correio.

   ```
   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 AWSDOC-
   EXAMPLE-BUCKET --s3-prefix S3-PREFIX
   ```

2. Use a AWS CLI para monitorar o estado dos trabalhos de exportação da caixa de correio para sua organização do Amazon WorkMail.

   ```
   aws workmail list-mailbox-export-jobs --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56
   ```

   Como alternativa, use o ID do trabalho gerado pelo comando **`start-mailbox-export-job`** para monitorar somente o estado desse trabalho de exportação de caixa de correio.

   ```
   aws workmail describe-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
   ```

Quando o estado do trabalho de exportação da caixa de correio estiver COMPLETED, os itens da caixa de correio exportados ficam disponíveis em um arquivo `.zip` no bucket especificado do Amazon S3.

Veja a seguir um exemplo de log de saída de caixa de correio exportada:

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportableItems são itens sem suporte, como notas e contatos.

Considerações

As seguintes considerações se aplicam à exportação de trabalhos de caixa de correio para o Amazon WorkMail:

- Você pode executar até 10 trabalhos simultâneos de exportação de caixas de correio para uma determinada organização do Amazon WorkMail.
- Você pode executar um trabalho de exportação de caixa de correio para uma determinada caixa de correio uma vez a cada 24 horas.
- Todos os recursos a seguir devem estar na mesma região da AWS:
  - Organização do Amazon WorkMail
  - CMK AWS KMS
  - Bucket do Amazon S3

Solução de problemas

Os tópicos desta seção explicam como solucionar problemas na Amazon WorkMail.

Tópicos

Visualizar cabeçalhos de e-mail

As informações nos cabeçalhos de e-mail podem ajudar a solucionar problemas de e-mail de usuários. A Amazon WorkMail permite que você visualize as informações do cabeçalho de qualquer mensagem.

Para visualizar cabeçalhos de e-mail na Amazon WorkMail

1. No aplicativo WorkMail web da Amazon, clique duas vezes na mensagem de e-mail para abri-la.
2. Selecione Opções de mensagem (o ícone de engrenagem e envelope) localizadas no canto superior direito da mensagem, ao lado da data de Envio.

Os cabeçalhos de e-mail aparecem em Internet Headers (Cabeçalhos da Internet).

Roteamento de correio

Se um usuário parar de receber e-mails, sua WorkMail organização da Amazon pode estar enfrentando um problema de roteamento de e-mails. As etapas desta seção explicam formas comuns de resolver problemas de entrega e roteamento.

Problemas com e-mails recebidos:

- Verifique o registro MX do domínio associado à sua WorkMail organização Amazon. `WorkMail`deve ser a única entrada e ter a prioridade mais baixa. Vários registros MX podem fazer com que o serviço errado receba mensagens. Para obter mais informações sobre registros MX, consulte Verificar domínios.
- Verifique as configurações de Autenticação, Relatórios e Conformidade de Mensagens Baseadas em Domínio (DMARC) para sua organização no console da Amazon. WorkMail Os registros

DMARC são usados para proteger contra ataques comuns, como falsificação ou phishing, que podem comprometer as credenciais da conta de um usuário. Para obter mais informações sobre DMARC, consulte Aplicar políticas DMARC em e-mails recebidos.

- Verifique a regra de entrada do Amazon Simple Email Service. Se a regra contiver ações diferentes da Amazon WorkMail, essas ações podem falhar e fazer com WorkMail que a Amazon pare de receber e-mails. Para obter mais informações sobre as regras do Amazon SES, consulte Integrar com a WorkMail ação da Amazon no Guia do desenvolvedor do Amazon Simple Email Service.
- Ative o rastreamento de mensagens na Amazon e WorkMail, em seguida, verifique se há problemas de entrega nos registros. Para obter mais informações sobre o rastreamento de mensagens, consulte Habilitando o registro de eventos de e-mail.

Problemas com e-mails enviados

- Certifique-se de que seu registro SPF inclua o Amazon SES. Verifique a página de domínios no WorkMail console da Amazon para verificar. Para obter mais informações sobre SPF, consulte Autenticar e-mail com SPF.
- Certifique-se de que WorkMail a Amazon tenha permissões para usar o domínio. Caso contrário, adicione o domínio novamente. Adicionar um domínio, neste guia, fornece o passo a passo.

Usando o registro no diário de e-mail com o Amazon WorkMail

É possível configurar o registro para registrar sua comunicação de email usando ferramentas integradas externas de arquivamento e eDiscovery. Isso garante que as regulamentações de conformidade de armazenamento de e-mails para proteção de privacidade, armazenamento físico de dados e proteção de informações sejam atendidas.

Usar o registro

O Amazon WorkMail registra todos os e-mail enviados para qualquer usuário na organização especificada e todas as mensagens enviadas pelos usuários dessa organização. Uma cópia de todos os e-mails é enviada para um endereço especificado pelo administrador do sistema no formato chamado `journal record`. Esse formato é compatível com os programas de e-mail da Microsoft. Não há cobrança adicional pelo registro de e-mail.

Dois endereços de e-mail são usados para o registro no diário de e-mail: um endereço de e-mail do registro e um do relatório. O endereço de e-mail de registro é o endereço de uma caixa postal dedicada ou de um dispositivo de terceiros integrado à sua conta, para o qual os relatórios de registro são enviados. O endereço de e-mail de relatório é o endereço do administrador do sistema, para o qual as notificações de erro de relatórios de registro são enviadas.

Todos os registros são enviados de um endereço de e-mail adicionado automaticamente ao seu domínio, que tem a seguinte aparência.

```
amazonjournaling@yourorganization.awsapps.com
```

Não há caixas de correio associadas a esse endereço, e não é possível criar uma usando esse nome ou endereço.

> **Note**
>
> não exclua o seguinte registro de domínio do console do Amazon Simple Email Service (Amazon SES) ou o registro no diário de e-mails deixará de funcionar.
>
> ```
> yourorganization.awsapps.com
> ```

Todos os e-mail recebidos e enviados geram um registro no diário, independentemente do número de destinatários ou grupos de usuário. Os e-mails que não gerarem um registro exibirão uma notificação de erro que é enviada para o endereço de e-mail de relatório.

Para habilitar o registro de e-mail

1. Abra o console do Amazon WorkMail em https://console.aws.amazon.com/workmail/.

   Se necessário, altere a região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações, consulte Regiões e endpoints da na Referência geral da Amazon Web Services.
2. No painel de navegação, selecione Organizações e escolha o nome da organização.
3. No painel de navegação, escolha Configurações da organização, escolha a guia Registro no diário e, sem seguida, escolha Editar.
4. Mova o controle deslizante Status do registro no diário para a posição ativado.
5. Em Endereço de e-mail de registro no diário, insira o endereço de e-mail fornecido pelo provedor de registro no diário de e-mail.

   > **Note**
   >
   > Recomendamos o uso de um provedor de registro dedicado.
6. Em Endereço de e-mail do relatório, insira o endereço de e-mail do administrador.
7. Escolha Save (Salvar). As alterações são aplicadas imediatamente.

Histórico do documento

A tabela a seguir descreve mudanças importantes em cada versão do Amazon WorkMail Administrator Guide. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

Alteração	Descrição	Data
Suporte ao registro de auditoria	Os registros de auditoria podem ser usados para monitorar o acesso do usuário às caixas de correio, auditar atividades suspeitas e depurar as configurações do provedor de disponibilidade e controle de acesso. Para obter mais informações, consulte Habilitar o registro de auditoria e o registro e monitoramento na Amazon WorkMail no Guia do WorkMail Administrador da Amazon.	20 de março de 2024
Suporte para Transport Layer Security (TLS)	A Amazon WorkMail interrompeu o suporte para Transport Layer Security (TLS) 1.0 e 1.1. Se você estiver usando o TLS 1.0 ou 1.1, deverá atualizar a versão do TLS para 1.2.	2 de novembro de 2023
Usuários remotos	Usuários remotos são WorkMail usuários da Amazon hospedados fora da WorkMail organização da Amazon ou hospedados em um domínio de e-mail diferente. Para obter mais informações, consulte	18 de setembro de 2023

	Usuários no Amazon WorkMail Administrator Guide.	
Acesso programático às caixas de correio	A Amazon WorkMail agora oferece funções de falsificação de identidade para conceder acesso programático às caixas de correio. Para obter mais informações, consulte Acesso programático às caixas de correio no Amazon WorkMail Administrator Guide.	04 de outubro de 2022
Configurar provedores de disponibilidade personalizados na Amazon WorkMail	A Amazon WorkMail oferece suporte ao uso de Provedores de Disponibilidade Personalizados (CAPs). Para obter mais informações, consulte Configurando um provedor de disponibilidade personalizado no Amazon WorkMail Administrator Guide.	30 de junho de 2022
Alterações no console para criar uma organização	A experiência WorkMail do console da Amazon para criar uma organização está atualizada. Para obter mais informações, consulte Criação de uma organização no Amazon WorkMail Administrator Guide.	23 de outubro de 2020

Exportar conteúdo da caixa de correio	Use a ação da `StartMailboxExportJob` API para exportar o conteúdo da WorkMail caixa de correio da Amazon para um bucket do Amazon Simple Storage Service (Amazon S3). Para obter mais informações, consulte Exportação do conteúdo da caixa de correio no Amazon WorkMail Administrator Guide.	22 de setembro de 2020
Políticas de retenção de caixa de correio	Defina políticas de retenção de caixas de correio para sua WorkMail organização Amazon que excluam automaticamente as mensagens de e-mail após um período de tempo que você escolher. Para obter mais informações, consulte Definindo políticas de retenção de caixas de correio no Amazon WorkMail Administrator Guide.	28 de maio de 2020

Ações de Execução de Lambda síncronas e assíncronas	Escolha configurações síncronas ou assíncronas para ações do Run Lambda nas regras de fluxo de e-mail da Amazon. WorkMail Para obter mais informações, consulte Configuração AWS Lambda para a Amazon WorkMail no Guia do WorkMail Administrador da Amazon.	11 de maio de 2020
Trabalhar com regras de controle de acesso	As regras de controle de acesso permitem que WorkMail os administradores da Amazon controlem como as caixas de correio de sua organização são acessadas. Para obter mais informações, consulte Como trabalhar com regras de controle de acesso no Amazon WorkMail Administrator Guide.	12 de fevereiro de 2020
Marcar uma organização	Marque uma WorkMail organização da Amazon para diferenciar as organizações no AWS Billing and Cost Management console ou para controlar o acesso aos recursos da organização. Para obter mais informações, consulte Como marcar uma organização no Amazon WorkMail Administrator Guide.	23 de janeiro de 2020

Aplicar políticas DMARC em e-mails recebidos	Para obter mais informaçõ es, consulte Aplicação de políticas de DMARC em e-mails recebidos no Amazon WorkMail Administrator Guide.	17 de outubro de 2019
Recuperar conteúdo de mensagens com o Lambda	Use a API Amazon WorkMail Message Flow com AWS Lambda para recuperar o conteúdo da mensagem. Para obter mais informaçõ es, consulte Recuperação do conteúdo da mensagem com o Lambda no WorkMail Amazon Administrator Guide.	12 de setembro de 2019
Registrando eventos WorkMail de e-mail da Amazon	Ative o registro de eventos por e-mail no WorkMail console da Amazon para rastrear mensagens de e-mail da sua organização. Para obter mais informações, consulte Mensagens de rastreamento no Amazon WorkMail Administrator Guide.	13 de maio de 2019
Inserção de registro DNS do Route 53	Ao configurar um domínio gerenciado em uma zona hospedada pública do Route 53, a Amazon insere WorkMail automaticamente os registros DNS para você. Para obter mais informações, consulte Adicionar um domínio no Amazon WorkMail Administrator Guide.	13 de fevereiro de 2019

Configurar o Lambda para ações de regra de e-mails recebidos	A Amazon WorkMail oferece suporte à configuração de funções do Lambda para uso com regras de fluxo de e-mail de entrada. Para obter mais informações, consulte Gerenciamento de fluxos de e-mail no Amazon WorkMail Administrator Guide.	24 de janeiro de 2019
Configurando o Lambda para Amazon WorkMail	A Amazon WorkMail oferece suporte à configuração de funções do Lambda para uso com regras de fluxo de e-mail de saída. Para obter mais informações, consulte Configurando o Lambda para a WorkMail Amazon no Guia do Administrador da WorkMail Amazon.	19 de novembro de 2018
Roteamento de SMTP	A Amazon WorkMail oferece suporte à configuração de gateways SMTP para uso com regras de fluxo de e-mail de saída. Para obter mais informações, consulte Configurando gateways SMTP no Amazon WorkMail Administrator Guide.	1 de novembro de 2018

Ferramentas de depuração de domínios personalizados	A Amazon WorkMail adicionou ferramentas de depuração para domínios personalizados. Para obter mais informaçõ es, consulte Adicionar um domínio no Amazon WorkMail Administrator Guide.	15 de outubro de 2018
Suporte ao Outlook 2019	A Amazon WorkMail oferece suporte ao Outlook 2019 para Windows e macOS. Para obter mais informaçõ es, consulte os requisito s de WorkMail sistema da Amazon no Amazon WorkMail Administrator Guide.	1º de outubro de 2018
Várias atualizações	Várias atualizações no layout do tópico e na organização.	12 de julho de 2018
Permissões da caixa de correio	Você pode usar as permissõe s de caixa de correio na Amazon WorkMail para conceder aos usuários ou grupos o direito de trabalhar nas caixas de correio de outros usuários. Para obter mais informaçõ es, consulte Como trabalhar com permissões de caixa de correio no Amazon WorkMail Administrator Guide.	9 de abril de 2018

Support for AWS CloudTrail	A Amazon WorkMail está integrada com AWS CloudTrail. Para obter mais informações, consulte Registrar chamadas de WorkMail API da Amazon AWS CloudTrail no Amazon WorkMail Administrator Guide.	12 de dezembro de 2017
Suporte a fluxos de e-mail	É possível configurar regras de fluxo de e-mail para lidar com o recebimento de e-mails com base no endereço de e-mail ou domínio de um remetente. Para obter mais informações, consulte Gerenciamento de fluxos de e-mail no Amazon WorkMail Administrator Guide.	5 de julho de 2017
Atualizações para Configuração Rápida	O Quick Setup agora cria um WorkMail diretório da Amazon para você. Para obter mais informações, consulte Configurar a Amazon WorkMail com configuração rápida no Guia do WorkMail administrador da Amazon.	10 de maio de 2017

Suporte a uma variedade maior de clientes de e-mail	Agora você pode usar a Amazon WorkMail com o Microsoft Outlook 2016 para Mac e clientes de e-mail IMAP. Para obter mais informações, consulte Requisitos de sistema para a Amazon WorkMail no Guia do WorkMail Administrador da Amazon.	9 de janeiro de 2017
Suporte ao registro SMTP	É possível configurar o registro para registrar uma comunicação de e-mail. Para obter mais informações, consulte Usando o diário de e-mail com a Amazon WorkMail no Amazon WorkMail Administrator Guide.	25 de novembro de 2016
Suporte ao redirecionamento de e-mails para endereços externos	É possível configurar regras de redirecionamento de e-mails atualizando a política de identidade do Amazon SES para seu domínio. Para obter mais informações, consulte Editar políticas de identidad e de domínio no Amazon WorkMail Administrator Guide.	26 de outubro de 2016

Suporte à interoperabilidade	Você pode ativar a interoperabilidade entre a Amazon e o WorkMail Microsoft Exchange. Para obter mais informações, consulte Interoperabilidade entre a Amazon e o WorkMail Microsoft Exchange no Guia do WorkMail Administrador da Amazon.	25 de outubro de 2016
Disponibilidade geral	A versão de disponibilidade geral da Amazon WorkMail.	4 de janeiro de 2016
Suporte à reserva de recursos	Suporte à reserva de recursos, como salas de reunião e equipamentos. Para obter mais informações, consulte Como trabalhar com recursos no Amazon WorkMail Administrator Guide.	19 de outubro de 2015
Suporte à ferramenta de migração de e-mails	Suporte à ferramenta de migração de e-mails. Para obter mais informações, consulte Migração para a Amazon WorkMail no Guia do WorkMail Administrador da Amazon.	16 de agosto de 2015
Versão prévia da Amazon WorkMail	A versão prévia da Amazon WorkMail.	28 de janeiro de 2015

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.