Guia de referência

AWS Gerenciamento de contas

AWS Gerenciamento de contas: Guia de referência

Table of Contents

Bem-vindo ao Guia de referência de gerenciamento de AWS contas

Contas da AWSsão uma parte fundamental do acesso aos AWS serviços.

E Conta da AWS tem duas funções básicas:

- Contêiner — Um Conta da AWS é o contêiner básico para todos os AWS recursos que você cria como AWS cliente. Por exemplo, um bucket do Amazon Simple Storage Service (Amazon S3), um banco de dados do Amazon Relational Database Service (Amazon RDS) e uma instância do Amazon Elastic Compute Cloud (Amazon EC2) são todos recursos. Cada recurso é identificado exclusivamente por um nome de recurso da Amazon (ARN) que inclui o ID da conta que contém ou é proprietária do recurso.
- Limite de segurança — Um também Conta da AWS é o limite básico de segurança para seus AWS recursos. Os recursos que você cria em sua conta estão disponíveis para usuários que têm credenciais para sua conta.

  Entre os principais recursos que você pode criar em sua conta estão identidades, como usuários e funções. As identidades têm credenciais que alguém pode usar para entrar (autenticar). AWS As identidades também têm políticas de permissão que especificam o que um usuário pode fazer (autorização) com os recursos na conta.

  Como prática recomendada de segurança, exija que seus usuários usem credenciais temporárias ao acessarAWS. Para fornecer credenciais temporárias, você pode usar a federação e um provedor de identidade, como AWS IAM Identity Center(IAM Identity Center). Se sua empresa já usa um provedor de identidade, use-o com federação para simplificar a forma como você fornece acesso aos recursos do seuConta da AWS.

  Para obter informações sobre as melhores práticas de segurança, consulte Melhores práticas de segurança no IAM no Guia do usuário do IAM.

Tópicos

Preciso de váriosContas da AWS?

Contas da AWSservem como o limite fundamental de segurança emAWS. Eles servem como um contêiner de recursos que fornece um nível útil de isolamento. A capacidade de isolar recursos e usuários é um requisito fundamental para estabelecer um ambiente seguro e bem governado.

Separando seus recursos em separadoContas da AWSajuda você a dar suporte aos seguintes princípios em seu ambiente de nuvem:

- Controle de segurança— Aplicativos diferentes podem ter perfis de segurança diferentes, exigindo diferentes políticas de controle e mecanismos ao seu redor. Por exemplo, é muito mais fácil falar com um auditor e poder apontar para um únicoConta da AWSque hospeda todos os elementos da sua carga de trabalho que estão sujeitos aPCI (Payment Card Industry) Padrões de segurança.
- Isolamento— UmConta da AWSé uma unidade de proteção de segurança. Riscos potenciais e ameaças à segurança devem estar contidos em umConta da AWSsem afetar os outros. Pode haver necessidades de segurança diferentes devido a diferentes equipes ou perfis de segurança diferentes.
- Muitas equipes— Diferentes equipes têm suas diferentes responsabilidades e necessidades de recursos. Você pode evitar que as equipes interfiram entre si, movendo-as para separarContas da AWS.
- Isolamento de dados— Além de isolar as equipes, é importante isolar os armazenamentos de dados em uma conta. Isso pode ajudar a limitar o número de pessoas que podem acessar e gerenciar esse armazenamento de dados. Isso ajuda a conter a exposição a dados altamente privados e, portanto, pode ajudar em conformidade com oGDPR — Regulamento geral de proteção de dados) da União Europeia.
- Processo de negócios— Unidades de negócios ou produtos diferentes podem ter propósitos e processos completamente diferentes. Com váriosContas da AWS, você pode suportar as necessidades específicas de uma unidade de negócios.
- Faturamento— Uma conta é a única maneira verdadeira de separar itens em um nível de faturamento. Várias contas ajudam a separar itens em um nível de faturamento em unidades de negócios, equipes funcionais ou usuários individuais. Você ainda pode consolidar todas as suas contas em um único pagador (usandoAWS Organizationse faturamento consolidado) enquanto tem itens de linha separados porConta da AWS.
- Alocação de cotas–AWScotas de serviço são aplicadas separadamente para cadaConta da AWS. Separando cargas de trabalho em diferentesContas da AWSos impede de consumir cotas um para o outro.

Todas as recomendações e procedimentos descritos neste documento estão em conformidade com oAWSEstrutura Well-Architected. Essa estrutura destina-se a ajudá-lo a projetar uma infraestrutura de nuvem flexível, resiliente e escalável. Mesmo quando você está começando pequeno, recomendamos que você continue em conformidade com essa orientação na estrutura. Isso pode ajudá-lo a dimensionar seu ambiente com segurança e sem afetar suas operações contínuas à medida que você cresce.

Gerenciar váriosContas da AWS

Antes de começar a adicionar várias contas, você vai querer desenvolver um plano para gerenciá-las. Para isso, recomendamos que você useAWS Organizations, o que é gratuitoAWSserviço para gerenciar todos osContas da AWSna organização.

AWStambém ofereceAWS Control Tower, que adiciona camadas deAWSautomação gerenciada para Organizations e integra-a automaticamente com outrosAWSServiços comoAWS CloudTrail,AWS Config, o Amazon CloudWatch,AWS Service Cataloge outros. Esses serviços podem implicar custos adicionais. Para obter mais informações, consulte Preço do AWS Control Tower.

Primeiros passos: Você é um AWS usuário iniciante?

Se você é um usuário iniciante doAWS, sua primeira etapa é se inscrever em umConta da AWS. Ao se inscrever, AWS cria um Conta da AWS com os detalhes fornecidos e atribui a conta a você. Depois de criar o seuConta da AWS, faça login como usuário raiz, ative a autenticação multifator (MFA) para o usuário raiz e atribua acesso administrativo a um usuário.

Etapas

- Pré-requisitos
- Etapa 1: Crie seu Conta da AWS
- Etapa 2: ativar o MFA para seu usuário root
- Etapa 3: criar um usuário administrador
- Tópicos relacionados

Pré-requisitos

Para se inscrever em umConta da AWS, você precisa das seguintes informações:

- Um nome de conta — O nome da conta aparece em vários lugares, como na sua fatura, e em consoles, como o painel Billing and Cost Management e o console. AWS Organizations

  Recomendamos que você use uma forma padrão de nomear suas contas para que você possa dar nomes fáceis de reconhecer. Para contas corporativas, considere usar um padrão de nomenclatura, como organização - propósito - ambiente (por exemplo, AnyCompany- auditoria - produção). Para contas pessoais, considere usar um padrão de nomenclatura, como nome - sobrenome - finalidade (por exemplo, paulo-santos-testaccount).

  Para obter informações sobre como alterar o nome de uma conta, consulte Como altero o nome na minhaConta da AWS? .
- Endereço — Se seu endereço de contato estiver na Índia, o contrato de usuário da sua conta é com Amazon Internet Services Private Limited (AISPL), um AWS vendedor local na Índia. É necessário fornecer o CVV como parte do processo de verificação. Talvez você também precise inserir uma senha de uso único, dependendo do seu banco. A AISPL cobra 2 INR do seu método de pagamento como parte do processo de verificação. A AISPL reembolsa esse valor após a conclusão da verificação.
- Endereço de e-mail — O endereço de e-mail é usado como nome de login do usuário root e é necessário para a recuperação da conta. Você deve ser capaz de receber mensagens de e-mail enviadas para esse endereço. Antes de realizar determinadas tarefas, você deve verificar se tem acesso ao e-mail enviado para esse endereço.

  > **Important**
  >
  > Se essa conta for para uma empresa, use uma lista de distribuição corporativa segura (por exemplo,`it.admins@example.com`) para que sua empresa possa manter o acesso a ela Conta da AWS mesmo quando um funcionário mudar de cargo ou sair da empresa. Como o endereço de e-mail pode ser usado para redefinir as credenciais do usuário raiz da conta, proteja o acesso a essa lista de distribuição ou endereço.
- Um número de telefone — Esse número pode ser usado para confirmar a propriedade da sua conta. Você deve ser capaz de receber chamadas nesse número de telefone.

> **Important**
>
> Se essa conta for para uma empresa, use um número de telefone corporativo para que sua empresa possa manter o acesso a ela Conta da AWS mesmo quando um funcionário mudar de cargo ou sair da empresa.

Etapa 1: Crie seu Conta da AWS

1. No seu navegador, abra a página AWS inicial.
2. Escolha Criar um Conta da AWS.

   > **Note**
   >
   > Se você AWS fez login recentemente, escolha Entrar. Se a opção Criar uma nova Conta da AWS não estiver visível, primeiro escolha Entrar em uma conta diferente e, em seguida, escolha Criar uma nova Conta da AWS.

3. Insira as informações da sua conta e escolha Verificar endereço de e-mail. Isso enviará um código de verificação para o endereço de e-mail especificado.
4. Insira seu código de verificação e escolha Verificar.
5. Insira uma senha forte para seu usuário root, confirme-a e escolha Continuar. AWSexige que sua senha atenda às seguintes condições:
   - Ter no mínimo 8 caracteres e no máximo 128 caracteres de extensão.
   - Incluir no mínimo três dos seguintes tipos de caracteres: maiúsculas, minúsculas, números e os símbolos ! @ # $ % ^ & * () <> [] {} | _+-=.
   - Não ser idêntica ao nome ou endereço de e-mail da sua Conta da AWS.
6. Escolha Comercial ou Pessoal. A diferença entre essas opções são as informações que solicitamos. Ambos os tipos de conta têm os mesmos recursos e funções.
7. Insira suas informações comerciais ou pessoais. Consulte as recomendações na seção Pré-requisitos sobre o endereço de e-mail e o número de telefone.
8. Leia e aceite o Contrato AWS do Cliente. Certifique-se de ler e entender os termos do Contrato do AWS Cliente.

9. Escolha Continue (Continuar). Nesse momento, você receberá uma mensagem de e-mail confirmando que Conta da AWS está pronto para uso. Você pode entrar na sua nova conta usando o endereço de e-mail e a senha fornecidos durante a inscrição. No entanto, você não pode usar nenhum AWS serviço até terminar de ativar sua conta.
10. Insira as informações sobre sua forma de pagamento. Se você quiser usar um endereço diferente para fins de cobrança, escolha Usar um novo endereço.
11. Escolha Verificar e continuar.
12. Insira o código do seu país ou região na lista e, em seguida, insira um número de telefone onde você possa ser contatado nos próximos minutos. Insira o código CAPTCHA e envie.
13. Quando o sistema automatizado entrar em contato com você, insira o PIN que você recebeu e envie.
14. Selecione seu AWS Support plano. Para obter uma descrição dos planos disponíveis, consulte Comparar AWS Support planos.
15. Escolha Concluir inscrição. É exibida uma página de confirmação indicando que sua conta está sendo ativada.
16. Verifique sua pasta de e-mail e spam para ver se há uma mensagem de e-mail que confirma que sua conta foi ativada. A ativação geralmente leva alguns minutos, mas às vezes pode levar até 24 horas.

    Depois de receber a mensagem de ativação, você terá acesso total a todos os AWS serviços.

> **Note**
>
> Se você estiver tendo problemas com a ativação da conta, consultethe section called “Problemas de criação de conta”.

Etapa 2: ativar o MFA para seu usuário root

É altamente recomendável que você ative o MFA para seu usuário root. O MFA reduz drasticamente o risco de alguém acessar sua conta sem sua autorização.

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

Para obter ajuda para fazer login usando seu usuário root, consulte Fazer login AWS Management Console como usuário root no Guia do usuário AWS de login.

2. Ative o MFA para seu usuário root.

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

Etapa 3: criar um usuário administrador

Como você não pode restringir o que um usuário raiz pode fazer, é altamente recomendável que você não use seu usuário raiz para nenhuma tarefa que não exija explicitamente o usuário raiz. Em vez disso, atribua acesso administrativo a um usuário administrativo no IAM Identity Center e faça login como esse usuário administrativo para realizar suas tarefas administrativas diárias.

Para obter instruções, consulte Configurar o Conta da AWS acesso para um usuário administrativo do IAM Identity Center no Guia do usuário do IAM Identity Center.

Tópicos relacionados

- Para obter informações sobre como proteger suas credenciais de usuário raiz, consulte Como proteger as credenciais do usuário raiz no Guia do usuário do IAM.
- Para ver uma lista de tarefas que exigem o usuário raiz, consulte Tarefas que exigem credenciais do usuário raiz no Guia do usuário do IAM.

Como usar a Usuário raiz da conta da AWS

> **Important**
>
> Qualquer pessoa que tenha credenciais de usuário raiz para sua Conta da AWS tem acesso irrestrito a todos os recursos de sua conta, inclusive informações de faturamento.

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os recursos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de email 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.

Para evitar o uso do usuário root nas tarefas diárias, saiba como configurar um usuário administrativo no AWS IAM Identity Center. Para obter recomendações adicionais de segurança do usuário root, consulte Melhores práticas do usuário root para seu Conta da AWS.

Você pode alterar ou redefinir a senha do usuário raiz e criar ou excluir chaves de acesso (IDs de chave de acesso e chaves de acesso secretas) para seu usuário raiz. Para obter ajuda para fazer login usando seu usuário root, consulte Fazer login AWS Management Console como usuário root no Guia do usuário AWS de login.

Gerencie seuConta da AWS

Esta seção inclui tópicos que descrevem como gerenciar seuConta da AWS.

> **Note**
>
> Se o seuConta da AWSfoi criado na Índia usandoAmazon Internet Services Private Limited(AISPL), há considerações adicionais. Para obter mais informações, consulte Gerenciar contas na Índia.

Tópicos

Crie um autônomo Conta da AWS

Este tópico descreve como criar um autônomo Conta da AWS que não seja gerenciado peloAWS Organizations. Se você quiser criar uma conta que faça parte de uma organização gerenciada porAWS Organizations, consulte Criação de uma conta de membro em sua organização no Guia do AWS Organizations usuário.

Essas instruções são para criar um ambiente Conta da AWS fora da Índia. Para criar uma conta na Índia, consulteCrie umConta da AWScom AISPL.

AWS Management Console

Para criar um Conta da AWS

1. Abra a página inicial da Amazon Web Services.
2. Escolha Criar um Conta da AWS.

> **Note**
>
> Se você AWS fez login recentemente, essa opção pode não estar lá. Em vez disso, escolha Entrar no console. Em seguida, se Criar uma nova Conta da AWS ainda não estiver visível, primeiro escolha Entrar em uma conta diferente e, em seguida, escolha Criar uma nova Conta da AWS.

3. Insira as informações da sua conta e escolha Verificar endereço de e-mail. Isso enviará um código de verificação para o endereço de e-mail especificado.

> **Important**
>
> Devido à natureza crítica do usuário raiz da conta, é altamente recomendável que você use um endereço de e-mail que possa ser acessado por um grupo, em vez de apenas por um indivíduo. Dessa forma, se a pessoa que se inscreveu Conta da AWS deixar a empresa, ela ainda Conta da AWS poderá ser usada porque o endereço de e-mail ainda está acessível.
> Se você perder o acesso ao endereço de e-mail associado aoConta da AWS, não poderá recuperar o acesso à conta caso perca a senha.

4. Insira seu código de verificação e escolha Verificar.
5. Insira uma senha forte para seu usuário root, confirme-a e escolha Continuar. AWSexige que sua senha atenda às seguintes condições:
   - Ter no mínimo 8 caracteres e no máximo 128 caracteres de extensão.
   - Incluir no mínimo três dos seguintes tipos de caracteres: maiúsculas, minúsculas, números e os símbolos ! @ # $ % ^ & * () <> [] {} | _+-=.
   - Não ser idêntica ao nome ou endereço de e-mail da sua Conta da AWS.
6. Escolha Comercial ou Pessoal. Contas pessoais e contas comerciais têm os mesmos recursos e funções.

7. Insira suas informações pessoais ou da empresa.

> **Important**
>
> Para empresasContas da AWS, é uma prática recomendada inserir:
>
> - Um número de telefone da empresa em vez de um número de telefone pessoal.
> - Um endereço de e-mail com um nome de domínio que pertence à empresa ou organização que usará a conta.
>
> Configurar o usuário raiz da conta com um endereço de e-mail individual ou um número de telefone pessoal pode tornar sua conta insegura.

8. Leia e aceite o Contrato AWS do Cliente. Certifique-se de ler e entender os termos do Contrato do AWS Cliente.
9. Escolha Continue (Continuar). Nesse momento, você receberá uma mensagem de e-mail confirmando que Conta da AWS está pronto para uso. Você pode entrar na sua nova conta usando o endereço de e-mail e a senha fornecidos durante a inscrição. No entanto, você não pode usar nenhum AWS serviço até terminar de ativar sua conta.
10. Insira as informações sobre sua forma de pagamento e escolha Verificar e continuar. Se você quiser usar um endereço de cobrança diferente para suas informações de AWS cobrança, escolha Usar um novo endereço.

    Você não pode continuar com o processo de inscrição até adicionar uma forma de pagamento válida.
11. Insira o código do seu país ou região na lista e, em seguida, insira um número de telefone onde você possa ser contatado nos próximos minutos.
12. Insira o código exibido no CAPTCHA e, em seguida, envie.
13. Quando o sistema automatizado entrar em contato com você, insira o PIN que você recebeu e envie.
14. Selecione um dos AWS Support planos disponíveis. Para obter uma descrição dos planos de Support disponíveis e seus benefícios, consulte Comparar AWS Support planos.
15. Escolha Concluir inscrição. É exibida uma página de confirmação indicando que sua conta está sendo ativada.

16. Verifique sua pasta de e-mail e spam para ver se há uma mensagem de e-mail que confirma que sua conta foi ativada. A ativação geralmente leva alguns minutos, mas às vezes pode levar até 24 horas.

    Depois de receber a mensagem de ativação, você terá acesso total a todos os AWS serviços.

AWS CLI & SDKs

Você pode criar contas de membros em uma organização gerenciada AWS Organizations executando a CreateAccountoperação enquanto estiver conectado à conta de gerenciamento da organização.

Você não pode criar uma operação autônoma Conta da AWS fora de uma organização usando uma operação AWS Command Line Interface (AWS CLI) ou de AWS API.

Exibir Conta da AWS identificadores

AWS atribui os seguintes identificadores exclusivos a cada um: Conta da AWS

Conta da AWS ID

Um número de 12 dígitos, como 012345678901, que identifica exclusivamente um. Conta da AWSMuitos AWS recursos incluem o ID da conta em seus Amazon Resource Names (ARNs). A parte do ID da conta distingue os recursos em uma conta dos recursos em outra conta. Se você for um usuário AWS Identity and Access Management (IAM), você pode entrar no AWS Management Console usando o ID da conta ou o alias da conta. Embora os IDs de conta, assim como qualquer informação de identificação, devam ser usados e compartilhados com cuidado, eles não são considerados informações secretas, sigilosas ou confidenciais.

ID de usuário canônica

Um identificador alfanumérico, como`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`, que é uma forma ofuscada do ID. Conta da AWS Você pode usar essa ID para identificar um Conta da AWS ao conceder acesso entre contas a buckets e objetos usando o Amazon Simple Storage Service (Amazon S3). Você pode recuperar o ID de usuário canônico para você Conta da AWS como usuário raiz ou usuário do IAM.

Você deve estar autenticado AWS para ver esses identificadores.

> **Warning**
>
> Não forneça suas AWS credenciais (incluindo senhas e chaves de acesso) a terceiros que precisem de seus Conta da AWS identificadores para compartilhar AWS recursos com você. Fazer isso daria a eles o mesmo acesso ao Conta da AWS que você tem.

Encontre seu Conta da AWS ID

Você pode encontrar o Conta da AWS ID usando o AWS Management Console ou o AWS Command Line Interface (AWS CLI). No console, a localização do ID da conta depende se você está conectado como usuário raiz ou usuário do IAM. O ID da conta é o mesmo se você estiver conectado como usuário raiz ou usuário do IAM.

Encontrando o ID da sua conta como usuário root

AWS Management Console

Para encontrar seu Conta da AWS ID quando estiver conectado como usuário root

> **Permissões mínimas**
>
> Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:
>
> - Ao fazer login como usuário raiz, você não precisa de nenhuma permissão do IAM.

1. Na barra de navegação no canto superior direito, escolha o nome ou o número da sua conta e, em seguida, escolha Credenciais de segurança.

   > **Tip**
   >
   > Se você não vê a opção de credenciais de segurança, você pode estar conectado como um usuário federado com uma função do IAM, em vez de como um usuário do IAM. Nesse caso, procure a conta de entrada e o número de identificação da conta ao lado dela.

2. Na seção Detalhes da conta, o número da conta aparece ao lado Conta da AWS do ID.

AWS CLI & SDKs

Para encontrar seu Conta da AWS ID usando o AWS CLI

> **Permissões mínimas**
>
> Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:
>
> - Ao executar o comando como usuário root, você não precisa de nenhuma permissão do IAM.

Use o comando get-caller-identity da seguinte forma.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Encontre o ID da sua conta como usuário do IAM

AWS Management Console

Para encontrar seu Conta da AWS ID quando estiver conectado como usuário do IAM

> **Permissões mínimas**
>
> Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:
>
> - `account:GetAccountInformation`

1. Na barra de navegação no canto superior direito, escolha seu nome de usuário e, em seguida, escolha Credenciais de segurança.

   > **Tip**
   >
   > Se você não vê a opção de credenciais de segurança, você pode estar conectado como um usuário federado com uma função do IAM, em vez de como um usuário do

IAM. Nesse caso, procure a conta de entrada e o número de identificação da conta ao lado dela.

2. Na parte superior da página, em Detalhes da conta, o número da conta aparece ao lado Conta da AWS do ID.

AWS CLI & SDKs

Para encontrar seu Conta da AWS ID usando o AWS CLI

> **Permissões mínimas**
>
> Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:
>
> - Ao executar o comando como usuário ou função do IAM, você deve ter:
> - `sts:GetCallerIdentity`

Use o comando get-caller-identity da seguinte forma.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Encontre o ID de usuário canônico para seu Conta da AWS

Você pode encontrar o ID de usuário canônico para Conta da AWS usar o AWS Management Console ou o. AWS CLIO ID de usuário canônico de um Conta da AWS é específico dessa conta. Você pode recuperar o ID de usuário canônico para você Conta da AWS como usuário raiz, usuário federado ou usuário do IAM.

Encontre o ID canônico como usuário raiz ou usuário do IAM

AWS Management Console

Para encontrar o ID de usuário canônico da sua conta quando estiver conectado ao console como usuário root ou usuário do IAM

> **Permissões mínimas**
>
> Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:
>
> - Ao executar o comando como usuário root, você não precisa de nenhuma permissão do IAM.
> - Ao fazer login como usuário do IAM, você deve ter:
> - `account:GetAccountInformation`

1. Faça login no AWS Management Console como usuário raiz ou usuário do IAM.
2. Na barra de navegação no canto superior direito, escolha o nome ou o número da sua conta e, em seguida, escolha Credenciais de segurança.

   > **Tip**
   >
   > Se você não vê a opção de credenciais de segurança, você pode estar conectado como um usuário federado com uma função do IAM, em vez de como um usuário do IAM. Nesse caso, procure a conta de entrada e o número de identificação da conta ao lado dela.

3. Na seção Detalhes da conta, a ID de usuário canônica aparece ao lado da ID de usuário canônica. Você pode usar seu ID de usuário canônico para configurar as listas de controle de acesso (ACLs) do Amazon S3.

AWS CLI & SDKs

Para encontrar o ID de usuário canônico usando o AWS CLI

O mesmo comando AWS CLI de API funciona para os Usuário raiz da conta da AWSusuários do IAM ou para as funções do IAM.

Use o comando list-buckets da seguinte maneira.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Encontre o ID canônico como um usuário federado com uma função do IAM

AWS Management Console

Para encontrar o ID canônico da sua conta quando estiver conectado ao console como um usuário federado com uma função do IAM

> **Permissões mínimas**
>
> - Você deve ter permissão para listar e visualizar um bucket do Amazon S3.

1. Faça login no AWS Management Console como um usuário federado com uma função do IAM.
2. No console do Amazon S3, escolha um nome de bucket para ver detalhes sobre um bucket.
3. Escolha a aba Permissões.
4. Na seção Lista de controle de acesso, em Proprietário do bucket, o ID canônico do seu Conta da AWS aparece.

AWS CLI & SDKs

Para encontrar o ID de usuário canônico usando o AWS CLI

O mesmo comando AWS CLI de API funciona para os Usuário raiz da conta da AWSusuários do IAM ou para as funções do IAM.

Use o comando list-buckets da seguinte maneira.

```
$ aws s3api list-buckets \
    --query Owner.ID \
```

```
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Atualize o Conta da AWS nome, endereço de e-mail ou senha do usuário root

Para editar seu Conta da AWS nome ou alterar a senha ou o endereço de e-mail do usuário root, execute as etapas do procedimento a seguir. Esse endereço de e-mail e senha são as credenciais que você usa para entrar como o. Usuário raiz da conta da AWS

> **Note**
>
> As alterações em um Conta da AWS podem levar até quatro horas para se propagar em todos os lugares.

AWS Management Console

Para editar seu Conta da AWS nome, senha do usuário root ou endereço de e-mail do usuário root

> **Permissões mínimas**
>
> Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:
>
> - Você deve fazer login como o Usuário raiz da conta da AWS, o que não requer permissões adicionais do IAM. Não é possível executar essas etapas como usuário ou perfil do IAM.

1. Use seu endereço Conta da AWS de e-mail e senha para fazer login no AWS Management Consolecomo seu Usuário raiz da conta da AWS.
2. No canto superior direito do console, selecione o nome ou número de sua conta e, em seguida, selecione Conta.
3. Na página Conta, ao lado de Configurações da conta, escolha Editar. Você será avisado para se autenticar novamente para fins de segurança.

> **Note**
>
> Se você não vir a opção Editar, é provável que você não esteja conectado como usuário raiz da sua conta. Não será possível modificar as configurações da conta enquanto estiver conectado como usuário ou perfil do IAM.

4. Na página Atualizar configurações da conta, escolha Editar ao lado do campo que você deseja atualizar.

   a. Para Nome — Na página Atualizar o nome da sua conta, em Novo nome da conta, insira o novo nome da conta e escolha Salvar alterações.

   > **Note**
   >
   > Se você não conseguir modificar o Conta da AWS nome, verifique se existe uma política de controle de serviço (SCP) AWS Organizations que restringe o acesso `account` ou está configurada para negar a `iam:UpdateAccountName` ação.

   b. Para e-mail — Na página Atualizar seu endereço de e-mail, preencha os campos Novo endereço de e-mail, Confirme o novo endereço de e-mail e confirme sua senha atual. Depois, escolha Salvar alterações. Um código de verificação é enviado para seu novo endereço de e-mail `deno-reply@verify.signin.aws`. Na página Verificar seu novo endereço de e-mail, em Código de verificação, insira o código que você recebeu do seu e-mail e escolha Salvar alterações.

   > **Note**
   >
   > O código de verificação pode levar até 5 minutos para chegar. Se você não vê o e-mail na sua caixa de entrada, verifique suas pastas de spam e lixo eletrônico.

   c. Para senha — Na página Atualizar sua senha, preencha os campos Senha atual, Nova senha e Confirmar nova senha. Depois, escolha Salvar alterações. Para obter orientações adicionais, incluindo as melhores práticas para definir senhas de usuário root, consulte Alterar a senha do Usuário raiz da conta da AWS no Guia do usuário do IAM.

5. Depois de fazer as alterações, selecione Done (Concluído).

AWS CLI & SDKs

Essa tarefa não é compatível com AWS CLI ou por uma operação de API de um dos AWS SDKs. Você pode executar essa tarefa somente usando AWS Management Console o.

Compreender os modos de operação da API

As operações de API que funcionam com umConta da AWSOs atributos do sempre funcionam em um dos dois modos de operação:

- Contexto individual— esse modo é usado quando um usuário ou função em uma conta acessa ou altera um atributo de conta namesma conta. O modo de contexto autônomo é usado automaticamente quando vocêDon't 't 'tincluir o`AccountId`parâmetro quando você chama um dos Account ManagementAWS CLIouAWSOperações do SDK.
- Contexto das Organizations— esse modo é usado quando um usuário ou função em uma conta em uma organização acessa ou altera um atributo de conta em uma conta de membro diferente na mesma organização. O modo de contexto da organização é usado automaticamente quando vocêfazerincluir o`AccountId`parâmetro quando você chama um dos Account ManagementAWS CLIouAWSOperação SDK. Você pode chamar as operações nesse modo somente a partir da conta de gerenciamento da organização ou da conta de administrador delegada para Gerenciamento de contas.

OAWS CLIeAWSAs operações do SDK podem funcionar tanto no contexto autônomo quanto no da organização.

- Se vocêDon't 't 'tincluir o`AccountId`, em seguida, a operação é executada no contexto autônomo e aplica automaticamente a solicitação à conta que você usou para fazer a solicitação. Isso é verdade se a conta for membro de uma organização ou não.
- Se você incluir o`AccountId`, em seguida, a operação é executada no contexto da organização e a operação funciona na conta Organizations especificada.
  - Se a conta que está chamando a operação for a conta de gerenciamento ou a conta de administrador delegada para o serviço de Gerenciamento de Contas, você poderá especificar qualquer conta membro dessa organização na`AccountId`parâmetro para atualizar a conta especificada do.
  - A única conta em uma organização que pode chamar uma das operações de contato alternativas e especificar seu próprio número de conta na`AccountId`é a conta especificada

como conta de administrador delegado para o serviço de Gerenciamento de contas. Qualquer outra conta, incluindo a conta de gerenciamento, recebe um `AccessDenied` exceção.

- Se você executar uma operação no modo independente, deverá ter permissão para executar a operação com uma política do IAM que inclua um `Resource` elemento de either `"*"` para permitir todos os recursos, ou um ARN que usa a sintaxe para uma conta autônoma.
- Se você executar uma operação no modo de organizações, deverá ter permissão para executar a operação com uma política do IAM que inclua um `Resource` elemento de either `"*"` para permitir todos os recursos, ou um ARN que usa a sintaxe de uma conta de membro em uma organização.

Concedendo permissões para atualizar atributos da conta

Como acontece com a maioria AWS operações, você concede permissões para adicionar, atualizar ou excluir atributos de conta para Contas da AWS ao usar o Políticas de permissões do IAM da. Ao anexar uma política de permissão do IAM a um principal do IAM (um usuário ou função), você especifica quais ações o principal pode realizar em quais recursos e em que condições.

A seguir estão algumas considerações específicas do Gerenciamento de Contas para criar uma política de permissões.

Formato do Nome de recurso da Amazon do Contas da AWS

- O Amazon Resource Name (ARN) para um Conta da AWS que você pode incluir na `resource` elemento de uma declaração de política é construído de forma diferente com base no fato de a conta que você deseja referenciar ser uma conta autônoma ou uma conta que está em uma organização. Consulte a seção anterior sobre Compreender os modos de operação da API.
  - Um ARN de conta para uma conta autônoma:

    ```
    arn:aws:account::{AccountId}:account
    ```

    Você deve usar esse formato ao executar uma operação de atributos de conta no modo independente, não incluindo o `AccountID` parâmetro .
  - Um ARN de conta para uma conta-membro de uma organização:

    ```
    arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
    ```

Você deve usar esse formato ao executar uma operação de atributos de conta no modo de organizações, incluindo o`AccountID`parâmetro .

Chaves de contexto para políticas do IAM

O serviço de gerenciamento de contas também oferece vários[Chaves de condição específicas do serviço de Gerenciamento de Contas](#)que fornecem controle refinado sobre as permissões concedidas.

`account:AccountResourceOrgPaths`

A chave de contexto`account:AccountResourceOrgPaths`permite que você especifique um caminho através da hierarquia da sua organização até uma unidade organizacional (OU) específica. Somente contas de membro contidas nessa OU correspondem à condição. O snippet de exemplo a seguir restringe a política a ser aplicada somente a contas que estão em uma das duas OUs especificadas.

Como`account:AccountResourceOrgPaths`é um tipo de cadeia de caracteres com vários valores, você deve usar o`ForAnyValue`ou`ForAllValues`[operadores de string de vários valores](#). Além disso, observe que o prefixo na chave de condição é`account`, mesmo que você esteja referenciando caminhos para OUs em uma organização.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgPaths": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
        ]
    }
}
```

`account:AccountResourceOrgTags`

A chave de contexto`account:AccountResourceOrgTags`permite que você faça referência às tags que podem ser anexadas a uma conta em uma organização. Uma tag é um par de cadeias de caracteres de chave/valor que você pode usar para categorizar e rotular os recursos em sua conta. Para obter mais informações sobre a atribuição de tags, consulte:[Tag Editor](#)noAWS Resource GroupsGuia do usuário do. Para obter informações sobre o uso de tags como parte de uma estratégia de controle de acesso baseada em atributos, consulte o[O que é ABAC para](#)

aAWSnoManual do usuário do IAM. O snippet de exemplo a seguir restringe a política a ser aplicada somente a contas em uma organização que tenham a tag com a chave.`projecte` um valor de ou de`blueoured`.

Como`account:AccountResourceOrgTags`é um tipo de cadeia de caracteres com vários valores, você deve usar o`ForAnyValueouForAllValues`operadores de string de vários valores. Além disso, observe que o prefixo na chave de condição é`account`, mesmo que você esteja referenciando as tags na conta de membro de uma organização.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgTags/project": [
            "blue",
            "red"
        ]
    }
}
```

> **Note**
>
> Você pode anexar tags somente a uma conta em uma organização. Você não pode anexar tags a um autônomoConta da AWS.

Atualize seuConta da AWSinformações de contato

Você pode armazenar informações de contato sobre ocontato da conta principalpara o seuConta da AWS. Você também pode adicionar ou editar informações de contato para:contatos alternativos da conta:

- Faturamento— O contato alternativo de cobrança receberá notificações relacionadas ao faturamento, como notificações de disponibilidade de faturas.
- Operações— O contato alternativo de operações receberá notificações relacionadas às operações.
- Segurança— O contato de segurança alternativo receberá notificações relacionadas à segurança, incluindo notificações doAWSEquipe de abuso.

Tópicos

- Atualize os contatos alternativos para o seu Conta da AWS
- Atualize o contato principal do seu Conta da AWS

Atualize os contatos alternativos para o seu Conta da AWS

Contatos alternativos AWS permitem entrar em contato com até três contatos alternativos associados à conta. Um contato alternativo não precisa ser uma pessoa específica. Em vez disso, você pode adicionar uma lista de distribuição de e-mail se tiver uma equipe que gerencia questões relacionadas a cobrança, operações e segurança. Eles são adicionais ao endereço de e-mail associado ao usuário raiz da conta. O contato principal da conta continuará recebendo todas as comunicações por e-mail enviadas para o e-mail da conta raiz.

Você pode especificar somente um de cada um dos seguintes tipos de contato associados a uma conta.

- Contato de cobrança
- Contato de operações
- Contato de segurança

Você pode adicionar ou editar contatos alternativos de forma diferente, dependendo se as contas são independentes ou fazem parte de uma organização:

- Autônomo Contas da AWS — Se Contas da AWS não estiver associado a uma organização, você pode atualizar seus próprios contatos alternativos usando o AWS Management Console ou via AWS CLI e SDKs. Para saber como fazer isso, consulte Atualizar contatos Conta da AWS alternativos autônomos.
- Contas da AWS dentro de uma organização — Para contas de membros que fazem parte de uma AWS organização, um usuário na conta de gerenciamento ou na conta de administrador delegado pode atualizar centralmente qualquer conta membro na organização a partir do AWS Organizations console ou programaticamente por meio da CLI AWS e dos SDKs. Para saber como fazer isso, consulte Atualizar contatos Conta da AWS alternativos em sua organização.

Tópicos

- Requisitos de número de telefone e endereço de e-mail
- Atualize os contatos alternativos para um autônomo Conta da AWS

- Atualize os contatos alternativos de qualquer um Conta da AWS em sua organização
- conta: chave de AlternateContactTypes contexto

Requisitos de número de telefone e endereço de e-mail

Antes de continuar com a atualização das informações de contatos alternativos da sua conta, recomendamos que você primeiro analise os seguintes requisitos ao inserir números de telefone e endereços de e-mail.

- Os números de telefone só podem conter números, espaços em branco e os seguintes caracteres:"". `+-()`
- Os endereços de e-mail podem ter até 254 caracteres e podem incluir os seguintes caracteres especiais na parte local do endereço de e-mail, além dos caracteres alfanuméricos padrão: `"+=.#|!&-_`".

Atualize os contatos alternativos para um autônomo Conta da AWS

Para adicionar ou editar os contatos alternativos para um autônomo Conta da AWS, execute as etapas no procedimento a seguir. O AWS Management Console procedimento abaixo sempre funciona somente no contexto autônomo. Você pode usar o AWS Management Console para acessar ou alterar somente os contatos alternativos na conta que você usou para chamar a operação.

AWS Management Console

Para adicionar ou editar os contatos alternativos para um autônomo Conta da AWS

> **Permissões mínimas**
>
> Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:
>
> - `account:GetAlternateContact`(para ver os detalhes de contato alternativos)
> - `account:PutAlternateContact`(para definir ou atualizar um contato alternativo)
> - `account:DeleteAlternateContact`(para excluir um contato alternativo)

1. Faça login no AWS Management Consolecomo um usuário ou função do IAM que tenha as permissões mínimas.
2. Escolha o nome da sua conta no canto superior direito da janela e, em seguida, escolha Conta.
3. Na página Conta, role para baixo até Contatos alternativos e, à direita do título, escolha Editar.

> **Note**
>
> Se você não vê a opção Editar, é provável que você não esteja conectado como usuário raiz da sua conta ou como alguém que tenha as permissões mínimas especificadas acima.

4. Altere os valores em qualquer um dos campos disponíveis.

> **Important**
>
> Para empresas Contas da AWS, é uma prática recomendada inserir o número de telefone e o endereço de e-mail da empresa, em vez de um pertencente a uma pessoa física.

5. Depois de fazer todas as alterações, escolha Atualizar.

AWS CLI & SDKs

Você pode recuperar, atualizar ou excluir as informações de contato alternativas usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

Observações

- Para realizar essas operações a partir da conta de gerenciamento ou de uma conta de administrador delegado em uma organização em relação às contas dos membros, você deve habilitar o acesso confiável ao serviço de conta.

Permissões mínimas

Para cada operação, você deve ter a permissão que mapeia para essa operação:

- `GetAlternateContact`(para ver os detalhes de contato alternativos)
- `PutAlternateContact`(para definir ou atualizar um contato alternativo)
- `DeleteAlternateContact`(para excluir um contato alternativo)

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de contato e conceder a outros a capacidade de ler e escrever.

Example

O exemplo a seguir recupera o contato alternativo de cobrança atual da conta do chamador.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

O exemplo a seguir define um novo contato alternativo de Operações para a conta do chamador.

```
$ aws account put-alternate-contact \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Example

> **Note**
>
> Se você realizar várias `PutAlternateContact` operações no mesmo Conta da AWS tipo de contato, a primeira adicionará o novo contato e todas as chamadas sucessivas para o mesmo Conta da AWS tipo de contato atualizarão o contato existente.

Example

O exemplo a seguir exclui o contato alternativo de segurança da conta do chamador.

```
$ aws account delete-alternate-contact \
    --alternate-contact-type=SECURITY
```

Se for bem-sucedido, esse comando não produzirá uma saída.

> **Note**
>
> Se você tentar excluir o mesmo contato mais de uma vez, o primeiro será bem-sucedido silenciosamente. Todas as tentativas posteriores geram uma `ResourceNotFound` exceção.

Atualize os contatos alternativos de qualquer um Conta da AWS em sua organização

Para adicionar ou editar os detalhes de contato alternativos de qualquer Conta da AWS pessoa em sua organização, execute as etapas do procedimento a seguir.

Requisitos

Para atualizar contatos alternativos com o AWS Organizations console, você precisa fazer algumas configurações preliminares:

- Sua organização deve habilitar todos os recursos para gerenciar as configurações em suas contas de membros. Isso permite o controle administrativo sobre as contas dos membros. Isso é definido por padrão quando você cria sua organização. Se sua organização estiver configurada somente para faturamento consolidado e você quiser habilitar todos os recursos, consulte Habilitando todos os recursos em sua organização.
- Você precisa habilitar o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulte Habilitar o acesso confiável para o gerenciamento de AWS contas.

> **Note**
>
> As políticas AWS Organizations gerenciadas `AWSOrganizationsReadOnlyAccess` ou `AWSOrganizationsFullAccess` são atualizadas para fornecer permissão para acessar as APIs de gerenciamento de AWS contas para que você possa acessar os dados da conta no AWS Organizations console. Para ver as políticas gerenciadas atualizadas, consulte Atualizações das políticas AWS gerenciadas da Organizations.

AWS Management Console

Para adicionar ou editar os contatos alternativos de qualquer um Conta da AWS em sua organização

1. Entre no AWS Organizations console com as credenciais da conta de gerenciamento da organização.
2. Contas da AWSEm, selecione a conta que você deseja atualizar.
3. Escolha Informações de contato e, em Contatos alternativos, localize o tipo de contato: contato de cobrança, contato de segurança ou contato de operações.

4. Para adicionar um novo contato, selecione Adicionar ou, para atualizar um contato existente, selecione Editar.
5. Altere os valores em qualquer um dos campos disponíveis.

> **Important**
>
> Para empresas Contas da AWS, é uma prática recomendada inserir o número de telefone e o endereço de e-mail da empresa, em vez de um pertencente a uma pessoa física.

6. Depois de fazer todas as alterações, escolha Atualizar.

AWS CLI & SDKs

Você pode recuperar, atualizar ou excluir as informações de contato alternativas usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Observações**
>
> - Para realizar essas operações a partir da conta de gerenciamento ou de uma conta de administrador delegado em uma organização em relação às contas dos membros, você deve habilitar o acesso confiável ao serviço de conta.
> - Você não pode acessar uma conta em uma organização diferente da que você está usando para chamar a operação.

> **Permissões mínimas**
>
> Para cada operação, você deve ter a permissão que mapeia para essa operação:
>
> - `GetAlternateContact`(para ver os detalhes de contato alternativos)

- `PutAlternateContact`(para definir ou atualizar um contato alternativo)
- `DeleteAlternateContact`(para excluir um contato alternativo)

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de contato e conceder a outros a capacidade de ler e escrever.

Example

O exemplo a seguir recupera o contato alternativo de cobrança atual da conta do chamador em uma organização. As credenciais usadas devem ser da conta de gerenciamento da organização ou da conta de administrador delegado do gerenciamento de contas.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING \
    --account-id 123456789012
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

O exemplo a seguir define o contato alternativo de Operações para a conta membro especificada em uma organização. As credenciais usadas devem ser da conta de gerenciamento da organização ou da conta de administrador delegado do gerenciamento de contas.

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
```

```
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Se for bem-sucedido, esse comando não produzirá uma saída.

> **Note**
>
> Se você realizar várias `PutAlternateContact` operações no mesmo Conta da AWS tipo de contato, a primeira adicionará o novo contato e todas as chamadas sucessivas para o mesmo Conta da AWS tipo de contato atualizarão o contato existente.

Example

O exemplo a seguir exclui o contato alternativo de segurança da conta membro especificada em uma organização. As credenciais usadas devem ser da conta de gerenciamento da organização ou da conta de administrador delegado do gerenciamento de contas.

```
$ aws account delete-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=SECURITY
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Example

> **Note**
>
> Se você tentar excluir o mesmo contato mais de uma vez, o primeiro será bem-sucedido silenciosamente. Todas as tentativas posteriores geram uma `ResourceNotFound` exceção.

conta: chave de AlternateContactTypes contexto

Você pode usar a chave de contexto `account:AlternateContactTypes` para especificar qual dos três tipos de cobrança é permitido (ou negado) pela política do IAM. Por exemplo, o exemplo a seguir de política de permissão do IAM usa essa chave de condição para permitir que os diretores

anexados recuperem, mas não modifiquem, somente o contato `BILLING` alternativo de uma conta específica em uma organização.

Como `account:AlternateContactTypes` é um tipo de sequência de caracteres de vários valores, você deve usar os operadores de cadeia de caracteres de vários valores `ForAnyValue` ou de `ForAllValues` vários valores.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "account:GetAlternateContact",
            "Resource": [
                "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "account:AlternateContactTypes": [
                        "BILLING"
                    ]
                }
            }
        }
    ]
}
```

Atualize o contato principal do seu Conta da AWS

Você pode atualizar as informações de contato primárias associadas à sua conta, incluindo nome completo do contato, nome da empresa, endereço postal, número de telefone e endereço do site.

Você edita o contato da conta principal de forma diferente, dependendo se as contas são independentes ou fazem parte de uma organização:

- Independente Contas da AWS — Se Contas da AWS não estiver associado a uma organização, você pode atualizar seu próprio contato de conta principal usando o AWS Management Console ou via AWS CLI e SDKs. Para saber como fazer isso, consulte Atualizar contato Conta da AWS primário autônomo.

- Contas da AWSdentro de uma organização — Para contas de membros que fazem parte de uma AWS organização, um usuário na conta de gerenciamento ou na conta de administrador delegado pode atualizar centralmente qualquer conta membro na organização a partir do AWS Organizations console ou programaticamente por meio da CLI AWS e dos SDKs. Para saber como fazer isso, consulte Atualizar o contato Conta da AWS principal em sua organização.

Tópicos

Requisitos de número de telefone e endereço de e-mail

Antes de continuar com a atualização das informações de contato principais da sua conta, recomendamos que você primeiro analise os seguintes requisitos ao inserir números de telefone e endereços de e-mail.

- Os números de telefone só podem conter números, espaços em branco e os seguintes caracteres:"". `+-()`
- Os números de telefone devem começar com o código do país + e não devem ter zeros à esquerda ou espaços adicionais após o código do país. Por exemplo, `+1` (EUA/Canadá) ou `+44` (Reino Unido).
- Os números de telefone devem incluir hífens "`-`" entre o código de área, o código de troca e o código local. Por exemplo, +1 202-555-0179.

> **Note**
>
> Os números de telefone inseridos sem hífens podem resultar na impossibilidade de receber chamadas durante o processo de verificação do número de telefone ao redefinir um dispositivo de MFA para o usuário root. Para obter mais informações, consulte Como faço para redefinir meu dispositivo de MFA de conta de usuário AWS raiz? .

- Por motivos de segurança, os números de telefone devem ser capazes de receber SMS deAWS. Números gratuitos não serão aceitos, pois a maioria não suporta SMS.
- Para empresasContas da AWS, é uma prática recomendada inserir o número de telefone e o endereço de e-mail da empresa, em vez de um pertencente a uma pessoa física. Configurar o

usuário raiz da conta com o endereço de e-mail ou número de telefone de um indivíduo pode dificultar a recuperação da sua conta se esse indivíduo deixar a empresa.

Atualizar o contato principal para um contato autônomo Conta da AWS

Para editar seus detalhes de contato principais para um autônomoConta da AWS, execute as etapas no procedimento a seguir. O AWS Management Console procedimento abaixo sempre funciona somente no contexto autônomo. Você pode usar o AWS Management Console para acessar ou alterar somente as informações de contato primárias da conta que você usou para chamar a operação.

AWS Management Console

Para editar seu contato principal para um contato autônomo Conta da AWS

> **Permissões mínimas**
>
> Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:
>
> - `account:GetContactInformation`(para ver os detalhes de contato principais)
> - `account:PutContactInformation`(para atualizar os detalhes de contato principais)

1. Faça login no AWS Management Consolecomo um usuário ou função do IAM que tenha as permissões mínimas.
2. Escolha o nome da sua conta no canto superior direito da janela e, em seguida, escolha Conta.
3. Role para baixo até a seção Informações de contato e, ao lado dela, escolha Editar.
4. Altere os valores em qualquer um dos campos disponíveis.
5. Depois de fazer todas as alterações, escolha Atualizar.

AWS CLI & SDKs

Você pode recuperar, atualizar ou excluir as informações de contato principais usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- GetContactInformation
- PutContactInformation

> **Observações**
>
> - Para realizar essas operações a partir da conta de gerenciamento ou de uma conta de administrador delegado em uma organização em relação às contas dos membros, você deve habilitar o acesso confiável ao serviço de conta.

> **Permissões mínimas**
>
> Para cada operação, você deve ter a permissão que mapeia para essa operação:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de contato e conceder a outros a capacidade de ler e escrever.

Example

O exemplo a seguir recupera as informações de contato primárias atuais da conta do chamador.

```
$ aws account get-contact-information
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
```

```
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

O exemplo a seguir define novas informações de contato primárias para a conta do chamador.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
 Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Atualize o contato principal de qualquer um Conta da AWS em sua organização

Para editar seus detalhes de contato principais Conta da AWS em qualquer um de sua organização, execute as etapas no procedimento a seguir.

Requisitos adicionais

Para atualizar o contato principal com o AWS Organizations console, você precisa fazer algumas configurações preliminares:

- Sua organização deve habilitar todos os recursos para gerenciar as configurações em suas contas de membros. Isso permite o controle administrativo sobre as contas dos membros. Isso é definido por padrão quando você cria sua organização. Se sua organização estiver configurada somente para faturamento consolidado e você quiser habilitar todos os recursos, consulte Habilitando todos os recursos em sua organização.
- Você precisa habilitar o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulte Habilitar o acesso confiável para o gerenciamento de AWS contas.

AWS Management Console

Para editar seu contato principal para qualquer pessoa Conta da AWS em sua organização

1. Entre no AWS Organizationsconsole com as credenciais da conta de gerenciamento da organização.
2. Contas da AWSEm, selecione a conta que você deseja atualizar.
3. Escolha Informações de contato e localize Contato principal,
4. Selecione Edit (Editar).
5. Altere os valores em qualquer um dos campos disponíveis.
6. Depois de fazer todas as alterações, escolha Atualizar.

AWS CLI & SDKs

Você pode recuperar, atualizar ou excluir as informações de contato principais usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- GetContactInformation
- PutContactInformation

> **Observações**
>
> - Para realizar essas operações a partir da conta de gerenciamento ou de uma conta de administrador delegado em uma organização em relação às contas dos membros, você deve habilitar o acesso confiável ao serviço de conta.
> - Você não pode acessar uma conta em uma organização diferente da que você está usando para chamar a operação.

> **Permissões mínimas**
>
> Para cada operação, você deve ter a permissão que mapeia para essa operação:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de contato e conceder a outros a capacidade de ler e escrever.

Example

O exemplo a seguir recupera as informações de contato primárias atuais da conta de membro especificada em uma organização. As credenciais usadas devem ser da conta de gerenciamento da organização ou da conta de administrador delegado do gerenciamento de contas.

```
$ aws account get-contact-information --account-id 123456789012
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

O exemplo a seguir define as informações de contato primárias da conta de membro especificada em uma organização. As credenciais usadas devem ser da conta de gerenciamento da organização ou da conta de administrador delegado do gerenciamento de contas.

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
 "CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
 "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Atualize as perguntas do desafio de segurança

As perguntas de desafio de segurança são um método de verificação usado anteriormente para verificar uma identidade em cenários de recuperação de conta. Eles são menos seguros do que as formas mais modernas de verificação, como a autenticação multifatorial (MFA). Se você atualmente tem perguntas de desafio de segurança ativas em sua conta Conta da AWS, AWS Support pode usá-las para ajudar a autenticá-lo como proprietário da conta.

> **Important**
>
> A partir de 5 de janeiro de 2024, não AWS haverá mais suporte para perguntas de desafio de segurança para contas que ainda não as habilitaram e usaram. Isso removerá a opção de adicionar novas perguntas de desafio de segurança da página Contas no AWS Management Console. Se você já definiu perguntas de desafio de segurança ou já as definiu na conta de gerenciamento AWS da sua organização, você pode continuar a usá-las. Depois de 6 de janeiro de 2025, não AWS oferecerá mais suporte às questões de desafio de segurança para todos os clientes restantes. Recomendamos que você adicione MFAem vez disso. Para obter mais informações, consulte Contas da AWS interrompe o uso de perguntas de desafio de segurança.

Para editar as perguntas de desafio de segurança existentes e fornecer as respostas, execute as etapas do procedimento a seguir.

AWS Management Console

Para editar perguntas de desafio de segurança para seu Conta da AWS

> **Permissões mínimas**
>
> Para executar as etapas a seguir, você deve ter pelo menos as seguintes IAM permissões:
>
> - `account:GetChallengeQuestions`(para ver as perguntas do desafio de segurança)

- `account:PutChallangeQuestions`(para definir ou atualizar as perguntas do desafio de segurança)

1. Faça login no AWS Management Consolecomo ou como IAM usuário Usuário raiz da conta da AWS ou função que tenha as permissões mínimas.
2. Escolha o nome da sua conta no canto superior direito da janela e, em seguida, escolha Conta.
3. Desça até a seção Perguntas do desafio de segurança e escolha Editar.

   > **Note**
   >
   > Se você não vê a opção Editar, é provável que você não esteja conectado como usuário raiz da sua conta ou como alguém que tenha as permissões mínimas especificadas acima.

4. Altere os valores em qualquer um dos campos disponíveis. Você pode selecionar qualquer uma das perguntas fornecidas e, em seguida, inserir a resposta adequada.
5. Depois de concluir suas alterações, escolha Atualizar.

AWS CLI & SDKs

Essa tarefa não é suportada no AWS CLI ou por uma API operação de um dos AWS SDKs. Você pode executar essa tarefa somente usando AWS Management Console o.

Especifique qual Regiões da AWS sua conta pode usar

An Região da AWSé um local físico no mundo em que temos várias zonas de disponibilidade. As zonas de disponibilidade consistem em um ou mais AWS data centers discretos, cada um com energia, rede e conectividade redundantes, alojados em instalações separadas. Isso significa que cada uma Região da AWS está fisicamente isolada e independente das outras regiões. As regiões fornecem tolerância a falhas, estabilidade e resiliência e também podem reduzir a latência. Para obter um mapa das regiões disponíveis e futuras, consulte Regiões e zonas de disponibilidade.

Os recursos que você cria em uma região não existem em nenhuma outra região, a menos que você use explicitamente um recurso de replicação oferecido por um AWS serviço. Por exemplo, o Amazon

S3 e o Amazon EC2 oferecem suporte à replicação entre Regiões. Alguns serviços, como AWS Identity and Access Management (IAM), não têm recursos regionais.

Sua conta determina as regiões que estão disponíveis para você.

- A An Conta da AWS fornece várias regiões para que você possa lançar AWS recursos em locais que atendam às suas necessidades. Por exemplo, talvez você queira lançar instâncias do Amazon EC2 na Europa para ficar mais perto de seus clientes europeus ou para atender aos requisitos legais.
- Uma conta AWS GovCloud (Oeste dos EUA) fornece acesso à região AWS GovCloud (Oeste dos EUA) e à região AWS GovCloud (Leste dos EUA). Para ter mais informações, consulte AWS GovCloud (US).
- Uma conta da Amazon AWS (China) fornece acesso somente às regiões de Pequim e Ningxia. Para obter mais informações, consulte Amazon Web Services na China.

Para obter uma lista de nomes de regiões e seus códigos correspondentes, consulte Endpoints regionais no Guia de referência AWS geral. Para obter uma lista dos AWS serviços suportados em cada região (sem endpoints), consulte a Lista de serviços AWS regionais.

> **Important**
>
> AWS recomenda que você use endpoints regionais AWS Security Token Service (AWS STS) em vez do endpoint global para reduzir a latência. Os tokens de sessão de AWS STS endpoints regionais são válidos em todas as AWS regiões. Se você usa AWS STS endpoints regionais, não precisa fazer nenhuma alteração. No entanto, os tokens de sessão do AWS STS endpoint global (https://sts.amazonaws.com) são válidos somente quando você ativa ou quando ativados por padrão. Regiões da AWS Se você pretende habilitar uma nova região para sua conta, você pode usar tokens de sessão de AWS STS endpoints regionais ou ativar o AWS STS endpoint global para emitir tokens de sessão que sejam válidos em todos. Regiões da AWS Os tokens de sessão válidos em todas as regiões são maiores. Se você armazenar tokens de sessão, esses tokens maiores podem afetar seus sistemas. Para obter mais informações sobre como AWS STS os endpoints funcionam com AWS regiões, consulte Gerenciando AWS STS em uma AWS região.

Tópicos

- Considerações antes de ativar e desativar regiões

- Ativar ou desativar uma região para contas autônomas
- Ativar ou desativar uma região em sua organização

Considerações antes de ativar e desativar regiões

Antes de ativar ou desativar uma região, é importante considerar o seguinte:

- As regiões introduzidas antes de 20 de março de 2019 estão habilitadas por padrão. AWS Originalmente, todas as novas são Regiões da AWS ativadas por padrão, o que significa que você pode começar a criar e gerenciar recursos nessas regiões imediatamente. Você não pode ativar ou desativar uma região que esteja ativada por padrão. Hoje, quando AWS adiciona uma região, a nova região é desativada por padrão. Se você quiser que seus usuários possam criar e gerenciar recursos em uma nova região, primeiro você precisa habilitar essa região. As seguintes regiões estão desativadas por padrão.

Nome	Código
Africa (Cape Town)	`af-south-1`
Ásia-Pacífico (Hong Kong)	`ap-east-1`
Ásia-Pacífico (Hyderabad)	`ap-south-2`
Ásia-Pacífico (Jacarta)	`ap-southeast-3`
Ásia-Pacífico (Melbourne)	`ap-southeast-4`
Canadá (Calgary)	`ca-west-1`
Europa (Milão)	`eu-south-1`
Europa (Espanha)	`eu-south-2`
Europa (Zurique)	`eu-central-2`
Israel (Tel Aviv)	`il-central-1`
Oriente Médio (Barém)	`me-south-1`

Nome	Código
Oriente Médio (Emirados Árabes Unidos)	`me-central-1`

- Você pode usar as permissões do IAM para controlar o acesso às regiões — AWS Identity and Access Management (IAM) inclui quatro permissões que permitem controlar quais usuários podem ativar, desativar, obter e listar regiões. Para obter mais informações, consulte AWS: Permite ativar e desativar Regiões da AWS no Guia do usuário do IAM. Você também pode usar a chave de `aws:RequestedRegion`condição para controlar o acesso Serviços da AWS em um Região da AWS.
- Habilitar uma região é gratuito — Não há cobrança para habilitar uma região. Você é cobrado somente pelos recursos criados na nova região.
- Desabilitar uma região desativa o acesso do IAM aos recursos na região — Se você desabilitar uma região que ainda contém AWS recursos, como instâncias do Amazon Elastic Compute Cloud (Amazon EC2), perderá o acesso do IAM aos recursos dessa região. Por exemplo, você não pode usar o AWS Management Console para visualizar ou alterar a configuração de nenhuma instância do EC2 em uma região desativada.
- As cobranças por recursos ativos continuam se você desativar uma região — Se você desabilitar uma região que ainda contém AWS recursos, as cobranças por esses recursos (se houver) continuarão sendo acumuladas na taxa padrão. Por exemplo, se você desabilitar uma região que contém instâncias do Amazon EC2, ainda precisará pagar as despesas relativas a essas instâncias, embora elas estejam inacessíveis.
- A desativação de uma região nem sempre é imediatamente visível — serviços e consoles podem ficar temporariamente visíveis após a desativação de uma região. A desativação de uma região pode levar de alguns minutos a várias horas para entrar em vigor.
- Habilitar uma região leva de alguns minutos a várias horas em alguns casos — Quando você ativa uma região, AWS realiza ações para preparar sua conta nessa região, como distribuir seus recursos do IAM para a região. Esse processo leva alguns minutos para a maioria das contas, mas às vezes pode levar várias horas. Você não pode usar a região até que esse processo seja concluído.
- As organizações podem ter 50 solicitações opcionais por região abertas em um determinado momento em toda a AWS organização — a conta de gerenciamento pode, a qualquer momento, ter 50 solicitações abertas pendentes de conclusão para sua organização. Uma solicitação equivale a ativar ou desativar uma região específica para uma conta.

- Uma única conta pode ter 6 solicitações de opção de região em andamento a qualquer momento — uma solicitação equivale a ativar ou desativar uma região específica para uma conta.
- EventBridge Integração com a Amazon — os clientes podem se inscrever para receber notificações de atualização de status por região em. EventBridge Uma EventBridge notificação será criada para cada mudança de status, permitindo que os clientes automatizem os fluxos de trabalho.
- Status expressivo de aceitação por região — devido à natureza assíncrona de ativar/desativar uma região de aceitação, há quatro possíveis status para uma solicitação de aceitação por região:
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  Você não pode cancelar um opt-in ou opt-out quando ele está em um ou outro `ENABLING` status. `DISABLING` Caso contrário, um `ConflictException` será lançado. Uma solicitação de opção de região concluída (ativada/desativada) depende do provisionamento dos principais serviços subjacentes. AWS Pode haver alguns AWS serviços que não serão imediatamente utilizáveis, apesar do status ser`ENABLED`.
- Integração total com AWS Organizations — Uma conta de gerenciamento pode modificar ou ler a região - optar por qualquer conta membro dessa AWS organização. Uma conta de membro também pode ler/gravar o estado de sua região.

Ativar ou desativar uma região para contas autônomas

Para atualizar as regiões às quais você Conta da AWS tem acesso, execute as etapas do procedimento a seguir. O AWS Management Console procedimento abaixo sempre funciona somente no contexto autônomo. Você pode usar o AWS Management Console para visualizar ou atualizar somente as regiões disponíveis na conta que você usou para chamar a operação.

AWS Management Console

Para ativar ou desativar uma região para um autônomo Conta da AWS

> **Permissões mínimas**
>
> Para realizar as etapas do procedimento a seguir, um usuário ou função do IAM deve ter as seguintes permissões:
>
> - `account:ListRegions`(necessário para ver a lista Regiões da AWS e se eles estão atualmente habilitados ou desativados).
> - `account:EnableRegion`
> - `account:DisableRegion`

1. Faça login no AWS Management Consolecomo usuário Usuário raiz da conta da AWS ou função do IAM que tenha as permissões mínimas.
2. Escolha o nome da sua conta no canto superior direito da janela e escolha Conta.
3. Na página Conta, role para baixo até a seção Regiões da AWS.

   > **Note**
   >
   > Você pode ser solicitado a aprovar seu acesso a essas informações. AWS envia uma solicitação para o endereço de e-mail associado à conta e para o número de telefone do contato principal. Escolha o link na solicitação para abri-lo em seu navegador e aprove o acesso.

4. Ao lado de cada um Região da AWS com uma opção na coluna Ação, escolha Ativar ou Desativar, dependendo se você deseja que os usuários da sua conta possam criar e acessar recursos nessa região.
5. Se solicitado, confirme sua escolha.
6. Depois de fazer todas as alterações, escolha Atualizar.

AWS CLI & SDKs

Você pode ativar, desativar, ler e listar o status de opção da região usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Permissões mínimas**
>
> Para executar as etapas a seguir, você deve ter a permissão que mapeia para essa operação:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de opção da região e conceder a outros a capacidade de ler e gravar.

O exemplo a seguir habilita uma região para a conta de membro especificada em uma organização. As credenciais usadas devem ser da conta de gerenciamento da organização ou da conta de administrador delegado do gerenciamento de contas.

Observe que você também pode desativar uma região usando o mesmo comando e depois `enable-region` substituindo por`disable-region`.

```
aws account enable-region --region-name af-south-1
```

Se for bem-sucedido, esse comando não produzirá uma saída.

A operação é assíncrona. O comando a seguir permitirá que você veja o status mais recente da solicitação.

```
aws account get-region-opt-status --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
```

```
}
```

Ativar ou desativar uma região em sua organização

Para atualizar as regiões habilitadas para suas contas de membros AWS Organizations, execute as etapas no procedimento a seguir.

> **Note**
>
> As políticas AWS Organizations gerenciadas `AWSOrganizationsReadOnlyAccess` ou `AWSOrganizationsFullAccess` são atualizadas para fornecer permissão para acessar as APIs de gerenciamento de AWS contas para que você possa acessar os dados da conta no AWS Organizations console. Para ver as políticas gerenciadas atualizadas, consulte Atualizações das políticas AWS gerenciadas da Organizations.

> **Note**
>
> Antes de realizar essas operações a partir da conta de gerenciamento ou de uma conta de administrador delegado em uma organização para uso com contas de membros, você deve:
>
> - Ative todos os recursos da sua organização para gerenciar as configurações em suas contas de membros. Isso permite o controle administrativo sobre as contas dos membros. Isso é definido por padrão quando você cria sua organização. Se sua organização estiver configurada somente para faturamento consolidado e você quiser habilitar todos os recursos, consulte Habilitando todos os recursos em sua organização.
> - Ative o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulteHabilitando acesso confiável para gerenciamento de AWS contas.

AWS Management Console

Para ativar ou desativar uma região em sua organização

1. Entre no AWS Organizations console com as credenciais da conta de gerenciamento da sua organização.
2. Na Contas da AWSpágina, selecione a conta que você deseja atualizar.

3. Escolha a guia Configurações da conta.
4. Em Regiões, selecione a região que você deseja ativar ou desativar.
5. Escolha Ações e escolha a opção Ativar ou Desativar.
6. Se você escolheu a opção Ativar, revise o texto exibido e escolha a região Ativar.
7. Se você escolheu a opção Desativar, revise o texto exibido, digite desabilitar para confirmar e escolha Desativar região.

AWS CLI & SDKs

Você pode ativar, desativar, ler e listar o status de opção da região para contas de membros da organização usando os seguintes AWS CLI comandos ou suas operações equivalentes de AWS SDK:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Permissões mínimas**
>
> Para executar as etapas a seguir, você deve ter a permissão que mapeia para essa operação:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações de opção da região e conceder a outros a capacidade de ler e gravar.

O exemplo a seguir habilita uma região para a conta de membro especificada em uma organização. As credenciais usadas devem ser da conta de gerenciamento da organização ou da conta de administrador delegado do gerenciamento de contas.

Observe que você também pode desativar uma região usando o mesmo comando e depois `enable-region` substituindo por`disable-region`.

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

Se for bem-sucedido, esse comando não produzirá uma saída.

> **Note**
>
> Uma organização só pode ter até 20 solicitações regionais em um determinado momento. Caso contrário, você receberá um`TooManyRequestsException`.

A operação é assíncrona. O comando a seguir permitirá que você veja o status mais recente da solicitação.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Crie ou atualize seu Conta da AWS alias

Se você quiser que o URL dos usuários do IAM contenha o nome da sua empresa (ou outro easy-to-remember identificador) em vez do Conta da AWS ID, você pode criar um alias de conta.

Para saber como criar ou atualizar um alias de conta, consulte Como criar, excluir e listar um Conta da AWS alias no Guia do usuário do IAM.

Faturamento para suaConta da AWS

Para procedimentos e tarefas relacionados ao faturamento relacionados à suaConta da AWS, consulte os tópicos a seguir noAWS Billing and Cost ManagementGuia do usuário do:

- Como alterar a moeda usada para pagar a fatura
- Como atualizar e excluir números de registro fiscal

- Como habilitar a herança de configurações de imposto

Gerenciar contas na Índia

Se você se inscrever em um novoConta da AWSe escolha a Índia como seu endereço de contato, seu contrato de usuário é comAmazon Internet Services Private Limited(AISPL), um localAWSO vendedor na Índia. O AISPL gerencia seu faturamento e o total da sua fatura é listado em rúpias indianas (INR) em vez de dólares americanos (USD). Depois que você criar uma conta com a AISPL, não será possível alterar o país nas suas informações de contato.

Se você tiver um existenteConta da AWScom um endereço na Índia, sua conta está comAWSou AISPL, dependendo de quando você abriu a conta. Para saber se sua conta está comAWSou AISPL, consulteDetermining which company your account is with. Se você já for um cliente existente da AWS, poderá continuar a usar sua conta da Conta da AWS. Você também pode optar por ter umConta da AWSe uma conta AISPL, embora não possam ser consolidados na mesmaAWSorganização. Para obter informações sobre como gerenciar umConta da AWS, vejaGerencie seuConta da AWS.

Se sua conta estiver com AISPL, siga os procedimentos neste tópico para gerenciar sua conta. Este tópico explica como se inscrever em uma conta AISPL, editar informações sobre sua conta AISPL e adicionar ou editar seu Número de Conta Permanente (PAN).

Como parte da verificação do cartão de crédito durante o cadastro, a AISPL faz uma cobrança de INR 2 no seu cartão de crédito. A AISPL reembolsa o INR 2 após a conclusão da verificação. Você pode ser redirecionado para seu banco como parte do processo de verificação.

Tópicos

Determine com qual empresa sua conta está

Os serviços da AWS são fornecidos pela AWS e pela AISPL. Use este procedimento para determinar em que vendedora sua conta está.

AWS Management Console

Para determinar em qual empresa sua conta está

> **Permissões mínimas**
>
> Para realizar as etapas a seguir, você deve ter pelo menos as seguintes permissões do IAM:
>
> - Esse procedimento não requer permissões especiais.

1. Abra o AWS Management Console em AWS Management Console.
2. No rodapé da página na parte inferior da página, veja o aviso de direitos autorais. Se os direitos autorais forem da Amazon Web Services, sua conta será da AWS. Se os direitos autorais forem da Amazon Internet Services Private Ltd., sua conta será da AISPL.

AWS CLI & SDKs

Essa tarefa não é suportada noAWS CLIou por uma operação de API de um dosAWSSDKs. Você pode executar essa tarefa somente usando oAWS Management Console.

Crie umConta da AWScom AISPL

AISPL é um vendedor local deAWSna Índia. Use o procedimento a seguir para se cadastrar em uma conta da AISPL, caso seu endereço de contato seja na Índia.

AWS Management Console

Para se cadastrar em uma conta da AISPL

> **Permissões mínimas**
>
> Para realizar as etapas a seguir, você deve ter pelo menos as seguintes permissões do IAM:
>
> - Porque essa operação ocorre antes de você ter umConta da AWS, esta operação não requerAWSpermissões.

1. Abra oAWS Management Consoleee, em seguida, escolhaFaça login no console.
2. Sobre oIniciar sessãopágina, insira o endereço de e-mail que você deseja usar.
3. No endereço de e-mail, selecione I am a new user e escolha Sign in using our secure server.
4. Para cada um dos campos de credencial de login, insira suas informações e escolhaCriar conta.
5. Para cada um dos campos de informações de contato, insira suas informações.
6. Após ler o acordo de cliente, marque a caixa de seleção dos termos e condições e escolha Create Account and Continue.
7. Na página Payment Information, informe o método de pagamento que você deseja usar.
8. AbaixoInformações do PAN, escolhaNãose você não tiver um Número de Conta Permanente (PAN) ou quiser adicioná-lo posteriormente. Se você tiver um PAN e quiser adicioná-lo agora, escolhasim, e noFRIGIDEIRAcampo insira seu PAN.
9. Escolha Verify Card and Continue. É necessário fornecer o CVV como parte do processo de verificação. A AISPL faz uma cobrança de INR 2 no seu cartão como parte do processo de verificação. A AISPL reembolsa o INR 2 após a conclusão da verificação.
10. ParaForneça um número de telefone, insira seu número de telefone. Se você tiver uma extensão telefônica, paraExt, insira sua extensão telefônica.
11. Escolha Call Me Now. Após alguns segundos, um PIN de quatro dígitos aparecerá na tela.
12. Aceite a chamada automática da AISPL. No teclado do telefone, insira o PIN de quatro dígitos exibido na tela.
13. Assim que a chamada automatizada verificar o número de contato, escolha Continue to Select Your Support Plan.
14. Na página Support Plan, selecione o plano de suporte e, em seguida, escolha Continue. Depois que sua forma de pagamento for verificada e sua conta ativada, você receberá uma mensagem de e-mail confirmando a ativação da sua conta.

AWS CLI & SDKs

Essa tarefa não é suportada noAWS CLIou por uma operação de API de um dosAWSSDKs. Você pode executar essa tarefa somente usando oAWS Management Console.

Gerencie sua conta AISPL

Com exceção das tarefas a seguir, os procedimentos para gerenciar sua conta são os mesmos das contas criadas fora da Índia. Consulte Gerencie seuConta da AWS.

Use oAWS Management Consolepara realizar as seguintes tarefas:

- Adicionar ou editar um número de conta permanente (PAN)
- Edite vários números de conta permanente (PANs)
- Edite vários números fiscais de bens e serviços (GSTs)
- Exibir uma nota fiscal

Fechar um Conta da AWS

Se você não precisar mais do seu Conta da AWS, poderá fechá-lo a qualquer momento seguindo as instruções nesta seção. Depois de fechá-la, você pode reabri-la dentro de 90 dias a partir do dia em que fechou a conta. O intervalo de tempo entre o dia em que você fechou a conta e o encerramento AWS permanente da conta é chamado de período pós-fechamento.

O que você precisa saber antes de fechar sua conta

Antes de fechar o seu Conta da AWS, você deve considerar o seguinte:

- O encerramento de sua conta servirá como seu aviso de rescisão do Contrato AWS do Cliente para essa conta.
- Você não precisa excluir recursos do seu Conta da AWS antes de fechá-lo. No entanto, recomendamos que você faça backup de todos os recursos ou dados que deseja manter. Para obter instruções sobre como fazer backup de um recurso específico, consulte a AWS documentação apropriada desse serviço.
- Você pode reabrir sua conta durante o período pós-encerramento. As cobranças pelos serviços que permaneceram em sua conta serão reiniciadas se você a reabrir. Você também permanece responsável por quaisquer faturas não pagas e por Instâncias Reservadas e Planos de Poupança pendentes.
- Você permanece responsável por todas as taxas e encargos pendentes pelos serviços consumidos antes do encerramento da conta. Você receberá uma AWS fatura no mês seguinte após o encerramento da conta. Por exemplo, se você fechou sua conta em 15 de janeiro,

receberá uma fatura no início de fevereiro pelo uso incorrido de 1º de janeiro a 15 de janeiro. Você continuará recebendo faturas de Reserved Instances and Savings Plans após fechar sua conta até que elas expirem.

- Você não poderá mais acessar os AWS serviços que estavam disponíveis anteriormente em sua conta. No entanto, você pode fazer login e acessar um arquivo fechado Conta da AWS durante o período pós-encerramento apenas para ver informações de cobrança anteriores, acessar as configurações da conta ou o contato. AWS Support
- Você não pode usar o mesmo endereço de e-mail que estava registrado Conta da AWS em seu nome no momento do encerramento como o e-mail principal de outra pessoa Conta da AWS. Se você quiser usar o mesmo endereço de e-mail para outro Conta da AWS, recomendamos atualizá-lo antes do encerramento. Consulte Atualize o Conta da AWS nome, endereço de e-mail ou senha do usuário root para obter instruções sobre como atualizar seu endereço de e-mail.
- Se você ativou a autenticação multifator (MFA) em seu usuário Conta da AWS root ou configurou um MFAdispositivo em um IAM usuário, ela MFA não é removida automaticamente quando você fecha a conta. Se você optar por deixar MFA ligado durante o período de 90 dias após o encerramento, mantenha o MFA dispositivo ativo até que o período pós-fechamento expire, caso você precise acessar a conta durante esse período. Observe que os dispositivos de TOTP token de hardware não podem ser associados a outro usuário após o encerramento permanente da sua conta. Se você quiser usar o TOTP token de hardware com outro usuário posteriormente, você tem a opção de desativar o MFA dispositivo de hardware antes de fechar a conta. MFAos dispositivos IAMdos usuários devem ser excluídos pelo administrador da conta.

Considerações adicionais para contas de membros

- Quando você fecha uma conta de membro, essa conta não é removida da organização até depois do período pós-encerramento. Durante o período pós-encerramento, uma conta de membro encerrada ainda será considerada na cota de contas na organização. Para evitar que a conta seja contabilizada na cota, consulte Remover uma conta membro da sua organização antes de fechá-la.
- Você só pode fechar 10% das contas dos membros em um período contínuo de 30 dias. Essa cota não está associada a um mês do calendário. A contagem começa assim que você encerra uma conta. Num prazo de 30 dias após o encerramento inicial da conta, você não poderá exceder o limite de 10% de encerramento da conta. O fechamento mínimo da conta é 10 e o fechamento máximo da conta é 1000, mesmo que 10% das contas excedam 1000. Para obter mais informações sobre cotas de Organizations, consulte Quotas para. AWS Organizations

- Se você usa o AWS Control Tower, precisa desgerenciar a conta do membro antes de tentar fechá-la. Consulte Unmanage a member account (Remover o gerenciamento de uma conta-membro) no Guia do usuário do AWS Control Tower.

Considerações específicas do serviço

- AWS Marketplace as assinaturas não são canceladas automaticamente no encerramento da conta. Se você tiver alguma assinatura, primeiro encerre todas as instâncias do seu software nas assinaturas. Em seguida, acesse a página Gerenciar assinaturas do AWS Marketplace console e cancele suas assinaturas.
- Depois que uma conta for fechada, AWS enviaremos e-mails diários por até cinco dias antes de suspendermos o domínio. Depois que o domínio for suspenso, e dependendo do registrador do domínio, excluiremos o domínio em 30 dias ou liberaremos o domínio para o registrador. Para obter mais informações, consulte Meu Conta da AWS está fechado ou fechado permanentemente e meu domínio está registrado no Route 53.
- AWS CloudTrail é um serviço de segurança fundamental. Isso significa que as trilhas criadas pelos usuários podem continuar existindo e entregando eventos mesmo após o fechamento de uma Conta da AWS , a menos que um usuário exclua explicitamente as trilhas Conta da AWS antes de fechá-las. Antes de fechar o seu Conta da AWS, considere o seguinte:
  - As trilhas continuam existindo mesmo após o término do período pós-fechamento. O período pós-fechamento se refere aos 90 dias entre o encerramento da conta e o encerramento AWS permanente da sua. Conta da AWS
  - Esse comportamento também se aplica às trilhas organizacionais criadas pela conta de gerenciamento ou pelo administrador delegado e às trilhas organizacionais multirregionais criadas nas contas dos membros da organização.
  - Para trilhas que entregam eventos para um bucket do S3 na mesma conta, as trilhas continuam existindo mesmo após o encerramento da conta. No entanto, como o bucket do S3 é excluído quando a conta é fechada, as trilhas não continuam entregando eventos.
  - Para trilhas que entregam eventos para um bucket do S3 em uma conta diferente, as trilhas continuam existindo mesmo após o encerramento da conta. As trilhas também continuam entregando eventos ao bucket do S3, se os eventos puderem ser entregues. Por exemplo, as trilhas da organização continuam entregando eventos ao bucket do S3 se você fechar uma conta membro em uma organização, mas não fechar a conta de gerenciamento.
  - Para trilhas criptografadas com AWS KMS keys, as trilhas continuam existindo após o encerramento da conta, além das KMS chaves.

Para obter mais informações e informações sobre como solicitar a exclusão de uma trilha após o fechamento de uma Conta da AWS , consulte Conta da AWS encerramento e trilhas no Guia do CloudTrail usuário.

Como fechar sua conta

Você pode fechar o seu Conta da AWS usando o procedimento a seguir. Observe que há orientações diferentes fornecidas em cada guia, dependendo do tipo de conta [autônoma, membro, gerencial e AWS GovCloud (US)] que você deseja fechar.

Se você tiver algum problema durante o processo de encerramento de sua conta, consulteSolução de problemas com o Conta da AWS fechamento.

Standalone account

Uma conta autônoma é uma conta gerenciada individualmente que não faz parte da AWS Organizations.

Para fechar uma conta independente na página Contas

1. Faça login no AWS Management Console como usuário root no Conta da AWS que você deseja fechar. Você não pode fechar uma conta enquanto estiver conectado como IAM usuário ou função.
2. Na barra de navegação no canto superior direito, escolha o nome ou o número da sua conta e, em seguida, escolha Conta.
3. Na página Conta, escolha o botão Fechar conta.
4. Digite o ID da sua conta (exibido na parte superior da caixa de diálogo de encerramento) para confirmar que você leu e entendeu o processo de encerramento da conta.
5. Escolha o botão Fechar conta para iniciar o processo de encerramento da conta.
6. Em alguns minutos, você receberá um e-mail de confirmação de que sua conta foi encerrada.

> **Note**
>
> Essa tarefa não é suportada no AWS CLI ou por uma API operação de um dos AWS SDKs. Você pode executar essa tarefa somente usando AWS Management Console o.

Member account

Uma conta de membro Conta da AWS faz parte de AWS Organizations.

Para fechar uma conta de membro a partir do AWS Organizations console

1. Faça login no console do AWS Organizations.
2. Na página Contas da AWS, localize e escolha o nome da conta-membro que deseja encerrar. É possível navegar na hierarquia da UO ou ver uma lista simples de contas sem a estrutura da UO.
3. Selecione Close (Encerrar) ao lado do nome da conta na parte superior da página. Organizações no modo de cobrança consolidada não conseguirão ver o botão Fechar no console. Para fechar uma conta no modo de cobrança consolidada, você precisará seguir as etapas na guia Conta independente.
4. Leia e certifique-se de entender as diretrizes de encerramento da conta.
5. Insira o ID da conta do membro e escolha Fechar conta para iniciar o processo de encerramento da conta.

Para fechar uma conta de membro na página Contas

Opcionalmente, você pode fechar uma conta de AWS membro diretamente da página Conta no AWS Management Console. Para step-by-step obter orientação, siga as instruções na guia Conta autônoma.

Para fechar uma conta de membro usando AWS CLI e SDKs

Para obter instruções sobre como fechar uma conta de membro usando o AWS CLI eSDKs, consulte Fechar uma conta de membro em sua organização no Guia do AWS Organizations usuário.

Management account

Uma conta de gerenciamento é Conta da AWS aquela que atua como conta principal ou raiz do AWS Organizations.

> **Note**
>
> Você não pode fechar uma conta de gerenciamento diretamente do AWS Organizations console.

Para fechar uma conta de gerenciamento na página Contas

1. Faça login AWS Management Console como usuário root da conta de gerenciamento que você deseja fechar. Você não pode fechar uma conta enquanto estiver conectado como IAM usuário ou função.
2. Verifique se não há contas de membros ativas restantes em sua organização. Para fazer isso, acesse o AWS Organizations console e verifique se todas as contas dos membros estão aparecendo `Suspended` ao lado dos nomes das contas. Se você tiver uma conta de membro que ainda esteja ativa, você precisará seguir as orientações de encerramento de conta fornecidas na guia Conta de membro antes de passar para a próxima etapa.
3. Na barra de navegação no canto superior direito, escolha o nome ou o número da sua conta e, em seguida, escolha Conta.
4. Na página Conta, escolha o botão Fechar conta.
5. Digite o ID da sua conta (exibido na parte superior da caixa de diálogo de encerramento) para confirmar que você leu e entendeu o processo de encerramento da conta.
6. Escolha o botão Fechar conta para iniciar o processo de encerramento da conta.
7. Em alguns minutos, você receberá um e-mail de confirmação de que sua conta foi encerrada.

> **Note**
>
> Essa tarefa não é suportada no AWS CLI ou por uma API operação de um dos AWS SDKs. Você pode executar essa tarefa somente usando AWS Management Console o.

AWS GovCloud (US) account

Uma AWS GovCloud (US) conta está sempre vinculada a um único padrão Conta da AWS para fins de cobrança e pagamento.

Para fechar uma AWS GovCloud (US) conta

Se você tem uma Conta da AWS que está vinculada a uma AWS GovCloud (US) conta, você precisa fechar a conta padrão antes de fechar a AWS GovCloud (US) conta. Para obter mais detalhes, incluindo como fazer backup de dados e evitar AWS GovCloud (US) cobranças não intencionais, consulte Fechar uma AWS GovCloud (US) conta no Guia do AWS GovCloud (US) usuário.

O que esperar depois de fechar sua conta

Imediatamente após você fechar sua conta, ocorrerá o seguinte:

- Você receberá um e-mail confirmando o encerramento da conta no endereço de e-mail do usuário root. Se você não receber esse e-mail em algumas horas, consulteSolução de problemas com o Conta da AWS fechamento.
- Qualquer conta de membro que você fechar exibirá uma `SUSPENDED` etiqueta ao lado do nome da conta no AWS Organizations console.
- Se você concedeu permissões para acessar serviços em suas Conta da AWS outras contas, qualquer solicitação de acesso feita a partir dessas contas deverá falhar após o encerramento da conta. Se você reabrir sua Conta da AWS, outras pessoas Contas da AWS poderão acessar novamente os AWS serviços e recursos da sua conta se você conceder as permissões necessárias a elas.

Período pós-encerramento

O período pós-fechamento se refere ao período de tempo entre o dia em que você fechou sua conta e o momento em que fecha AWS permanentemente sua. Conta da AWS O período pós-fechamento é de 90 dias. Durante o período pós-encerramento, você só pode acessar seu conteúdo e AWS serviços reabrindo sua conta. Após o período pós-fechamento, fecha AWS permanentemente o seu Conta da AWS e você não poderá mais reabri-lo. AWS também excluirá qualquer conteúdo e recursos da sua conta. Depois que uma conta for encerrada permanentemente, seu Conta da AWS ID nunca poderá ser reutilizado.

Reabrindo seu Conta da AWS

Sua conta será encerrada permanentemente em 90 dias, após os quais você não poderá reabrir sua conta e AWS excluirá o conteúdo restante em sua conta. Para reabrir sua conta antes que ela seja encerrada permanentemente, (1) você deve entrar em contato o mais rápido AWS Supportpossível e (2) devemos receber o pagamento integral de qualquer saldo pendente, incluindo o fornecimento das informações necessárias conforme especificado na fatura, dentro de 60 dias a partir da data de encerramento da conta.

> **Note**
>
> As cobranças pelos serviços que permaneceram em sua conta serão reiniciadas se você a reabrir.

Usando o gerenciamento de AWS contas em sua organização

AWS Organizationsé um AWS serviço que você pode usar para gerenciar seu Contas da AWS grupo. Isso fornece recursos como o faturamento consolidado, em que todas as contas de suas contas são agrupadas e administradas por um único pagador. Você também pode gerenciar centralmente a segurança da sua organização usando controles baseados em políticas. Para obter mais informações sobre o AWS Organizations, consulte o Guia do usuário do AWS Organizations.

Acesso confiável

Quando você usa AWS Organizations para gerenciar suas contas como um grupo, a maioria das tarefas administrativas da organização pode ser executada somente pela conta de gerenciamento da organização. Por padrão, isso inclui somente operações relacionadas ao gerenciamento da própria organização. Você pode estender essa funcionalidade adicional para outros AWS serviços, permitindo o acesso confiável entre as organizações e esse serviço. O acesso confiável concede permissões ao AWS serviço especificado para acessar informações sobre a organização e as contas que ela contém. Quando você habilita o acesso confiável para o Gerenciamento de Contas, o serviço de Gerenciamento de Contas concede às organizações e suas contas de gerenciamento permissões para acessar os metadados, como as informações de contato primárias ou alternativas, de todas as contas dos membros da organização.

Para obter mais informações, consulte Habilitando acesso confiável para gerenciamento de AWS contas.

Administrador delegado

Depois de ativar o acesso confiável, você também pode escolher designar uma de suas contas de membro como uma conta de administrador delegado para AWS o Gerenciamento de Contas. Isso permite que a conta de administrador delegado execute as mesmas tarefas de gerenciamento de metadados do Gerenciamento de Contas para as contas dos membros em sua organização que anteriormente somente a conta de gerenciamento podia fazer. A conta de administrador delegado pode acessar somente as tarefas de gerenciamento do serviço de gerenciamento de contas. A conta de administrador delegado não tem todo o acesso administrativo à organização que a conta de gerenciamento tem.

Para obter mais informações, consulte Habilitar uma conta de administrador delegado para oAWSGerenciamento de contas.

Políticas de controle de serviço

Quando você Conta da AWS faz parte de uma organização gerenciada porAWS Organizations, o administrador da organização pode aplicar políticas de controle de serviços (SCPs) que podem limitar o que os diretores nas contas dos membros podem fazer. Um SCP nunca concede permissões; em vez disso, é um filtro que limita quais permissões podem ser usadas pela conta do membro. Um usuário ou função (um principal) em uma conta de membro pode realizar somente as operações que estão na interseção do que é permitido pelos SCPs que se aplicam à conta e às políticas de permissão do IAM anexadas ao principal. Por exemplo, você pode usar SCPs para impedir que qualquer administrador de uma conta modifique os contatos alternativos de sua própria conta.

Por exemplo, SCPs que se aplicam aContas da AWS, consulteRestringir acesso comAWS OrganizationsPolíticas de controle de serviço.

Habilitando acesso confiável para gerenciamento de AWS contas

Habilitar o acesso confiável ao Gerenciamento de Contas permite que o administrador da conta de gerenciamento modifique as informações e os metadados (por exemplo, detalhes de contato primários ou alternativos) específicos de cada conta de membro emAWS Organizations. AWS Para obter mais informações, consulte Gerenciamento de AWS contas e AWS Organizations no Guia AWS Organizations do usuário. Para obter informações gerais sobre como o acesso confiável funciona, consulte Uso AWS Organizations com outros AWS serviços.

Depois que o acesso confiável for ativado, você poderá usar o `accountID` parâmetro nas operações da API de gerenciamento de contas que o suportam. Você pode usar esse parâmetro com êxito somente se chamar a operação usando credenciais da conta de gerenciamento ou da conta de administrador delegado da sua organização, se você habilitar uma. Para obter mais informações, consulte Habilitar uma conta de administrador delegado para oAWSGerenciamento de contas.

Use o procedimento a seguir para habilitar o acesso confiável para o Gerenciamento de Contas em sua organização.

> **Permissões mínimas**
>
> Para realizar essas tarefas, você deve atender aos seguintes requisitos:
>
> - Você pode fazer isso somente na conta de gerenciamento da organização.

- A organização deve ter todos os recursos habilitados.

AWS Management Console

Para habilitar o acesso confiável para o gerenciamento de AWS contas

1. Faça login no console do AWS Organizations. É necessário fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário root (não recomendado) na conta de gerenciamento da organização.
2. Escolha Serviços no painel de navegação.
3. Escolha Gerenciamento de AWS contas na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para gerenciamento de AWS contas, digite enable para confirmá-lo e escolha Habilitar acesso confiável.

AWS CLI & SDKs

Para habilitar o acesso confiável para o gerenciamento de AWS contas

Depois de executar o comando a seguir, você pode usar as credenciais da conta de gerenciamento da organização para chamar as operações da API de gerenciamento de contas que usam o `--accountId` parâmetro para referenciar contas de membros em uma organização.

- AWS CLI: enable-aws-service-access

  O exemplo a seguir permite o acesso confiável para o gerenciamento de AWS contas na organização da conta chamadora.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Se for bem-sucedido, esse comando não produzirá uma saída.

Habilitar uma conta de administrador delegado para oAWSGerenciamento de contas

Uma conta de administrador delegada pode chamar oAWSOperações da API de gerenciamento de contas-membro para outras contas-membro na organização. Para designar uma conta de membro em sua organização como uma conta de administrador delegada, use o procedimento a seguir.

> **Permissões mínimas**
>
> Para executar essas tarefas, você deve atender aos seguintes requisitos:
>
> - É possível fazer isso somente a partir da conta de gerenciamento da organização.
> - A organização deve ter todos os recursos habilitados.
> - Você deve terhabilitou o acesso confiável para o Gerenciamento de contas em sua organização.

Depois de especificar uma conta de administrador delegada para sua organização, os usuários e as funções nessa conta podem chamar oAWS CLIeAWSOperações do SDK no`account`namespace que pode funcionar no modo Organizations, dando suporte a um opcional`AccountId`parâmetro .

AWS Management Console

Essa tarefa não tem suporte noAWSConsole de gerenciamento de gerenciamento de conta. É possível executar essa tarefa somente usando oAWS CLIou uma operação de API de um dosAWSSDKs.

AWS CLI & SDKs

Para registrar uma conta de administrador delegado para o serviço de Gerenciamento de contas

Você pode usar os seguintes comandos para habilitar um admin delegado para o serviço de Gerenciamento de conta.

É necessário especificar a seguinte entidade de serviço:

```
account.amazonaws.com
```

- AWS CLI:registrador-delegado administrador

O exemplo a seguir registra uma conta de membro da organização como um administrador delegado para o serviço de Gerenciamento de contas.

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

Esse comando não produz saída se for bem-sucedido.

Depois de executar esse comando, você pode usar as credenciais da conta 123456789012 para chamar o Gerenciamento de ContaAWS CLIe operações da API SDK que usam o`--account-id`Para referenciar contas-membro em uma organização.

Restringir acesso comAWS OrganizationsPolíticas de controle de serviço

Este tópico apresenta exemplos que mostram como usar políticas de controle de serviço (SCPs - service control policies) para restringir o que os usuários e as funções nas contas-na sua organização podem fazer. Para obter mais informações sobre políticas de controle de serviço, consulte os tópicos a seguir noAWS OrganizationsGuia do usuário do:

- Criar SCPs
- Anexando SCPs a OUs e contas
- Estratégias para SCPs
- Sintaxe da política SCP

Example Exemplo 1: Impedir que as contas modifiquem seus próprios contatos alternativos

O exemplo a seguir nega a`PutAlternateContact`e`DeleteAlternateContact`As operações de API não sejam chamadas por qualquer conta de membro emmodo de conta autônoma. Isso impede que qualquer principal nas contas afetadas altere seus próprios contatos alternativos.

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

```
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "arn:aws:account::*:account" ]
        }
    ]
}
```

Example Exemplo 2: Impedir que qualquer conta de membro modifique contatos alternativos para qualquer outra conta de membro na organização

O exemplo a seguir generaliza o`Resource`elemento para “*”, o que significa que se aplica a ambossolicitações de modo autônomo e solicitações do modo de organizações. Isso significa que mesmo a conta de administrador delegada para Gerenciamento de Contas, se o SCP se aplicar a ela, está impedida de alterar qualquer contato alternativo para qualquer conta na organização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "*" ]
        }
    ]
}
```

Example Exemplo 3: Impedir que uma conta de membro em uma OU modifique seus próprios contatos alternativos

O exemplo de SCP a seguir inclui uma condição que compara o caminho da organização da conta com uma lista de duas OUs. Isso resulta no bloqueio de um principal em qualquer conta nas OUs especificadas de modificar seus próprios contatos alternativos.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": "account:PutAlternateContact",
            "Resource": [
                "arn:aws:account::*:account"
            ],
            "Condition": {
                "ForAnyValue:StringLike": {
                    "account:AccountResourceOrgPath": [
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/",
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
                    ]
                }
            }
    ]
}
```

Segurança emAWSGerenciamento de contas

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

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

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Gerenciamento de contas, consulteServiços da AWSem escopo pelo programa de conformidade.
- Segurança da nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e os regulamentos aplicáveis

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar oAWSGerenciamento de contas. Ela mostra como configurar o Gerenciamento de contas para atender aos objetivos de segurança e conformidade. Você também saberá mais sobre como usar outrosAWSServiços da que ajudam a monitorar e proteger os recursos do Gerenciamento de contas.

Tópicos

Proteção de dados no gerenciamento de AWS contas

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados no gerenciamento de AWS contas. 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 obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

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 a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as 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 FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

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 o Gerenciamento de Contas ou outro Serviços da AWS usando o console,API, AWS CLI, ou AWS SDKs. 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, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

AWS PrivateLinkpeloAWSGerenciamento de contas

Se você usar o Amazon Virtual Private Cloud (Amazon VPC) para hospedar oAWSRecursos, é possível acessar oAWSServiço de gerenciamento de contas de dentro da VPC sem ter que atravessar a internet pública.

A Amazon VPC permite iniciar recursos da AWS em uma rede virtual personalizada. Você pode usar uma VPC para controlar as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Para obter informações sobre como criar suas próprias VPCs, consulte o Guia do usuário da Amazon VPC.

Para conectar sua Amazon VPC ao Gerenciamento de contas, você deve primeiro definir umVPC endpoint de interface, o que permite conectar sua VPC a outroAWSServiços da . O endpoint fornece conectividade confiável e escalável sem a necessidade de um gateway da Internet, da instância de conversão de endereço de rede (NAT) ou de uma conexão VPN. Para obter mais informações, consulte Endpoints da VPC da interface (AWS PrivateLink) no Guia do usuário da Amazon VPC.

Criação do endpoint

É possível criar umAWSEndpoint de gerenciamento de contas em sua VPC usando oAWS Management Console, oAWS Command Line Interface(AWS CLI), umAWSSDK, oAWSAPI de gerenciamento de contas ouAWS CloudFormation.

Para obter informações sobre como criar e configurar um endpoint usando o console da Amazon VPC ou aAWS CLI , consulte Creating an Interface Endpoint (“Criar um endpoint da interface”) no Manual do usuário da Amazon VPC.

> **Note**
>
> Ao criar um endpoint, especifique Gerenciamento de contas como o serviço ao qual a VPC deve se conectar, usando o formato a seguir:
>
> ```
> com.amazonaws.us-east-1.account
> ```

Você deve usar a string exatamente como mostrado, especificando `ous-east-1`Região : Como um serviço global, o Gerenciamento de contas é hospedado apenas nesseAWSRegião :

Para obter informações sobre como criar e configurar um endpoint usando o AWS CloudFormation, consulte o recurso AWS::EC2::VPCEndpoint no Manual do usuário do AWS CloudFormation.

Políticas de Endpoint da Amazon VPC

Você pode controlar quais ações podem ser executadas por meio desse endpoint de serviço anexando uma política de endpoint ao criar o endpoint da Amazon VPC. É possível criar regras do IAM complexas anexando várias políticas de endpoint. Para obter mais informações, consulte:

- Políticas de endpoint da Amazon Virtual Private Cloud para Gerenciamento de contas
- Controle do acesso a serviços com VPC endpointsnoAWS PrivateLinkGuia.

Políticas de endpoint da Amazon Virtual Private Cloud para Gerenciamento de contas

É possível criar uma política de endpoint da Amazon VPC para Gerenciamento de contas na qual se especifica o seguinte:

- A entidade principal que pode executar ações.
- As ações que os diretores podem executar.
- O recurso no qual as ações podem ser executadas.

O exemplo a seguir mostra uma política de endpoint da Amazon VPC que permite que um usuário do IAM chamado Alice na conta 123456789012 recupere e altere as informações de contato alternativas para qualquerConta da AWS, mas nega a todos os usuários do IAM permissão para excluir qualquer informação de contato alternativa em qualquer conta.

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

```
                "account:GetAlternateContact",
                "account:PutAlternateContact"
            ],
            "Resource": "arn:aws::iam:*:account,
            "Effect": "Allow",
            "Principal": {
              "AWS": "arn:aws::iam:123456789012:user/Alice"
            }
        },
        {
            "Action": "account:DeleteAlternateContact",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "arn:aws::iam:*:root"
        }
    ]
}
```

Se quiser conceder acesso às contas que fazem parte de umAWSOrganização para um principal que esteja em uma das contas de membros da organização, depois o`Resource`O elemento deve usar o seguinte formato::

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Para obter mais informações sobre como criar políticas de endpoint, consulteControle do acesso a serviços com VPC endpointsnoAWS PrivateLinkGuia.

Identity and Access Management para gerenciamento de AWS contas

AWS Identity and Access Management (IAM) é uma ferramenta Serviço da AWS que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar os recursos de gerenciamento de contas. IAMé um Serviço da AWS que você pode usar sem custo adicional.

Tópicos

- Como o gerenciamento de AWS contas funciona com IAM
- Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS
- Usando políticas baseadas em identidade (IAMpolíticas) para AWS gerenciamento de contas
- Solução de problemas de identidade e acesso ao gerenciamento de AWS contas

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Gerenciamento de contas.

Usuário do serviço — Se você usar o serviço de gerenciamento de contas para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões necessárias. À medida que você usa mais recursos de gerenciamento de contas para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Gerenciamento de contas, consulteSolução de problemas de identidade e acesso ao gerenciamento de AWS contas.

Administrador de serviços — Se você é responsável pelos recursos de gerenciamento de contas em sua empresa, provavelmente tem acesso total ao gerenciamento de contas. É seu trabalho determinar quais recursos e recursos de gerenciamento de contas seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar o Gerenciamento IAM de Contas, consulteComo o gerenciamento de AWS contas funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Gerenciamento de contas. Para ver exemplos de políticas baseadas em identidade de gerenciamento de contas que você pode usar emIAM, consulte. Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS

Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do 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 entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. 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 em 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 você mesmo assinar solicitações, consulte Assinar AWS API solicitações no Guia IAM do usuário.

Independente 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 e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

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 puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade.

Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no Guia do AWS IAM Identity Center usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham 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 IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. 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 IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

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 IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções 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 obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura 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 uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente 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 funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- 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 aplicativos na 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 a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações 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 FAS solicitações, consulte Encaminhar sessões de acesso.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.

- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível ao armazenamento de chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando 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 JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas 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 permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar 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 do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

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

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente 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 Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem 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 um principal especificado 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 localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

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

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, consulte a 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 recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas 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 suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no Guia AWS Organizations 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 atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

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 política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como o gerenciamento de AWS contas funciona com IAM

Antes de usar IAM para gerenciar o acesso ao Gerenciamento de contas, saiba quais IAM recursos estão disponíveis para uso com o Gerenciamento de contas.

IAMrecursos que você pode usar com o gerenciamento de AWS contas

IAMrecurso	Suporte ao gerenciamento de contas
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC(tags nas políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para ter uma visão geral de como o gerenciamento de contas e outros AWS serviços funcionam com a maioria dos IAM recursos, consulte AWS os serviços que funcionam com IAM no Guia do IAM usuário.

Políticas baseadas em identidade para gerenciamento de contas

Compatível com políticas baseadas em identidade: Sim

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

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para gerenciamento de contas

Para ver exemplos de políticas baseadas em identidade de gerenciamento de contas, consulte. Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS

Políticas baseadas em recursos no gerenciamento de contas

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem 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 um principal especificado 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

Para habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um IAM administrador na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Ações políticas para gerenciamento de contas

Compatível com ações de políticas: Sim

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

O `Action` elemento de uma JSON política 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 AWS API operação associada. Há algumas exceções, como ações somente de permissão que não têm uma operação correspondente. API Algumas operações também 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.

Para ver uma lista de ações de gerenciamento de contas, consulte Ações definidas pelo gerenciamento de AWS contas na Referência de autorização de serviço.

As ações de política no Gerenciamento de contas usam o seguinte prefixo antes da ação.

```
account
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "account:action1",
      "account:action2"
         ]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que funcionam com os contatos alternativos Conta da AWS de um, inclua a ação a seguir.

```
"Action": "account:*AlternateContact"
```

Para ver exemplos de políticas baseadas em identidade de gerenciamento de contas, consulte. Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS

Recursos de políticas para gerenciamento de contas

Compatível com recursos de políticas: Sim

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

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

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

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

O serviço de gerenciamento de contas oferece suporte aos seguintes tipos de recursos específicos no `Resources` elemento de uma IAM política para ajudá-lo a filtrar a política e distinguir entre esses tipos de Contas da AWS:

- conta

  Esse `resource` tipo corresponde apenas a contas autônomas Contas da AWS que não são membros em uma organização gerenciada pelo AWS Organizations serviço.
- accountInOrganization

  Esse `resource` tipo corresponde apenas Contas da AWS às contas de membros em uma organização gerenciada pelo AWS Organizations serviço.

Para ver uma lista dos tipos de recursos de gerenciamento de contas e seusARNs, consulte Recursos definidos pelo gerenciamento de AWS contas na Referência de autorização de serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo gerenciamento de AWS contas. ARN

Para ver exemplos de políticas baseadas em identidade de gerenciamento de contas, consulte. Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS

Chaves de condição de política para gerenciamento de contas

Compatível com chaves de condição de política específicas de serviço: Sim

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

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia IAM do usuário.

O serviço de gerenciamento de contas oferece suporte às seguintes chaves de condição que você pode usar para fornecer uma filtragem refinada para suas políticas: IAM

- conta: TargetRegion

Essa chave de condição usa um argumento que consiste em uma lista de códigos de AWS região. Ele permite que você filtre a política para afetar somente as ações que se aplicam às regiões especificadas.

- conta: AlternateContactTypes

  Essa chave de condição usa uma lista de tipos de contato alternativos:

  - BILLING
  - OPERATIONS
  - SECURITY

  O uso dessa chave permite filtrar a solicitação somente para as ações que têm como alvo os tipos de contato alternativos especificados.

- conta: AccountResourceOrgPaths

  Essa chave de condição usa um argumento que consiste em uma lista ARNs com curingas que representam contas em uma organização. Ele permite que você filtre a política para afetar somente as ações direcionadas às contas com ARNs essa correspondência. Por exemplo, o seguinte ARN corresponde somente às contas na organização especificada e na unidade organizacional (OU) especificada.

  ```
  arn:aws:account::111111111111:ou/o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- conta: AccountResourceOrgTags

  Essa chave de condição usa um argumento que consiste em uma lista de chaves e valores de tag. Ele permite filtrar a política para afetar somente as contas que são membros de uma organização e que estão marcadas com as chaves e valores de tag especificados.

Para ver uma lista das chaves de condição de gerenciamento de contas, consulte Chaves de condição para gerenciamento de AWS contas na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo gerenciamento de AWS contas.

Para ver exemplos de políticas baseadas em identidade de gerenciamento de contas, consulte. Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS

Listas de controle de acesso no Gerenciamento de contas

SuportesACLs: Não

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

Controle de acesso baseado em atributos com gerenciamento de contas

Suportes ABAC (tags nas políticas): Sim

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitos AWS recursos. Marcar entidades e recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usando credenciais temporárias com o gerenciamento de contas

Compatível com credenciais temporárias: Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS esse trabalho IAM no Guia do IAM usuário.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias emIAM.

Permissões principais entre serviços para gerenciamento de contas

Suporta sessões de acesso direto (FAS): Sim

Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações 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 FAS solicitações, consulte Encaminhar sessões de acesso.

Funções de serviço para gerenciamento de contas

Compatível com perfis de serviço: não

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.

Funções vinculadas a serviços para gerenciamento de contas

Compatível com perfis vinculados ao serviço: Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao

serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte AWS serviços que funcionam com. IAM Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos de gerenciamento de contas. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte Criação de IAM políticas no Guia do IAMusuário.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Gerenciamento de Contas, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para Gerenciamento de AWS Contas na Referência de Autorização de Serviço. ARNs

Tópicos

Melhores práticas de política

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

- Comece com políticas AWS gerenciadas e avance para permissões de privilégios mínimos — Para começar a conceder permissões para 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 obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas 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 usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica Serviço da AWS, como AWS CloudFormation. Para obter mais informações, consulte elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Usando a página Conta no AWS Management Console

Para acessar a página Conta no AWS Management Console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas exigidas, o console não funcionará conforme planejado para entidades (IAMusuários ou funções) com essa política.

Para garantir que usuários e funções possam usar o console de gerenciamento de contas, você pode optar por anexar a política `AWSAccountManagementReadOnlyAccess` ou a política `AWSAccountManagementFullAccess` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do IAM usuário.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, em muitos casos, você pode optar por permitir o acesso somente às ações que correspondem às API operações que você está tentando realizar.

Fornecendo acesso somente para leitura à página Conta no AWS Management Console

No exemplo a seguir, você deseja conceder a um IAM usuário em seu acesso Conta da AWS somente para leitura à página Conta no. AWS Management Console Os usuários com essa política anexada não podem fazer alterações.

A `account:GetAccountInformation` ação concede acesso para visualizar a maioria das configurações na página Conta. No entanto, para visualizar as AWS regiões atualmente habilitadas, você também deve incluir a `account:ListRegions` ação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantReadOnlyAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Fornecendo acesso total à página Conta no AWS Management Console

No exemplo a seguir, você deseja conceder a um IAM usuário acesso Conta da AWS total à página Conta no AWS Management Console. Os usuários com essa política anexada podem alterar as configurações da conta.

Esse exemplo de política se baseia no exemplo anterior, adicionando cada uma das permissões de gravação disponíveis (com exceção de CloseAccount), o que permite ao usuário alterar a maioria das configurações da conta, incluindo as permissões `account:EnableRegion` e. `account:DisableRegion`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutChallengeQuestions",
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

Usando políticas baseadas em identidade (IAMpolíticas) para AWS gerenciamento de contas

Para uma discussão completa sobre Contas da AWS e IAM usuários, consulte O que éIAM? no Guia do IAM usuário.

Para obter instruções sobre como atualizar as políticas gerenciadas pelo cliente, consulte Edição de políticas gerenciadas pelo cliente (console) no Guia IAM do usuário.

AWS Políticas de ações de gerenciamento de contas

Esta tabela resume as permissões que concedem acesso às configurações da sua conta. Para exemplos de políticas que usam essas permissões, consulte exemplos de políticas de gerenciamento de AWS contas.

> **Note**
>
> Para conceder IAM aos usuários acesso de gravação a uma configuração de conta específica na página Conta do AWS Management Console, você deve conceder a `GetAccountInformation` permissão, além da permissão (ou permissões) que deseja usar para modificar essa configuração.

Nome da permissão	Nível de acesso	Descrição
`account:ListRegions`	Listar	Concede permissão para listar as regiões disponíveis.
`account:GetAccountInformation`	Leitura	Concede permissão para recuperar as informações da conta.
`account:GetAlternateContact`	Leitura	Concede permissão para recuperar os contatos alternativos de uma conta.
`account:GetChallengeQuestions`	Leitura	Concede permissão para recuperar as perguntas do desafio de uma conta.
`account:GetContactInformation`	Leitura	Concede permissão para recuperar as principais informações de contato de uma conta.

Nome da permissão	Nível de acesso	Descrição
`account:GetRegionOptStatus`	Leitura	Concede permissão para obter o status de opt-in de uma região.
`account:AcceptPrimaryEmailUpdate`	Escrever	Concede permissão para aceitar a atualização do endereço de e-mail principal da conta do membro em uma AWS organização.
`account:CloseAccount`	Escrever	Concede permissão para fechar uma conta. **Note** Esta é uma permissão somente para o console. Não há API acesso disponível para essa permissão.
`account:DeleteAlternateContact`	Escrever	Concede permissão para excluir os contatos alternativos de uma conta.
`account:DisableRegion`	Escrever	Concede permissão para desativar o uso de uma região.
`account:EnableRegion`	Escrever	Concede permissão para permitir o uso de uma região.
`account:PutAlternateContact`	Escrever	Concede permissão para modificar os contatos alternativos de uma conta.

Nome da permissão	Nível de acesso	Descrição
`account:PutChallengeQuestions`	Escrever	Concede permissão para modificar as perguntas do desafio de uma conta. **Note** Esta é uma permissão somente para o console. Não há API acesso disponível para essa permissão.
`account:PutContactInformation`	Escrever	Concede permissão para atualizar as informações de contato principais de uma conta.
`account:StartPrimaryEmailUpdate`	Escrever	Concede permissão para iniciar a atualização do endereço de e-mail principal da conta do membro em uma AWS organização.

Solução de problemas de identidade e acesso ao gerenciamento de AWS contas

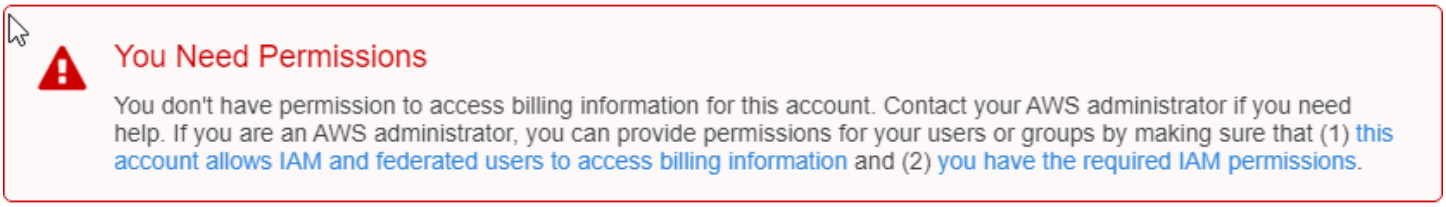
Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Gerenciamento de Contas e. IAM

Tópicos

Não estou autorizado a realizar uma ação na página Conta

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 `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre ele Conta da AWS na página Conta do AWS Management Console , mas não tem as `account:GetAccountInformation` permissões.



Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *`my-example-widget`* usando a ação `account:`*`GetWidget`*.

Não estou autorizado a executar **`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 o Gerenciamento de contas.

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 IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação no Gerenciamento de contas. 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 acessem Conta da AWS os detalhes da minha conta

Você pode criar um perfil 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 o Gerenciamento de Contas oferece suporte a esses recursos, consulteComo o gerenciamento de AWS contas funciona com IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

AWSpolíticas gerenciadas paraAWSGerenciamento de contas

AWSAtualmente, o Gerenciamento de Contas fornece doisAWSpolíticas gerenciadas que estão disponíveis para seu uso:

- Política gerenciada da AWS: AWSAccountManagementReadOnlyAccess
- Política gerenciada da AWS: AWSAccountManagementFullAccess
- Atualizações do gerenciamento de contas paraAWSpolíticas gerenciadas

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para todos os clientes da

AWS usarem. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo Serviço da AWS é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Política gerenciada da AWS: AWSAccountManagementReadOnlyAccess

É possível anexar a política `AWSAccountManagementReadOnlyAccess` a suas identidades do IAM.

Essa política fornece permissões somente de leitura para visualizar somente o seguinte:

- Os metadados sobre seuContas da AWS
- ORegiões da AWSque estão habilitados ou desativados para oConta da AWS(você pode ver o status das regiões em sua conta somente usando oAWSconsole)

Ele faz isso concedendo permissão para executar qualquer um dos`Get*`ou`List*`operações. Ele não oferece nenhuma capacidade de modificar os metadados da conta, ativar ou desativarRegiões da AWSpara a conta.

Detalhes da permissão

Esta política inclui as seguintes permissões.

- `account`— Permite que os diretores recuperem as informações de metadados sobreContas da AWS. Também permite que os diretores listem oRegiões da AWSque estão habilitados para a conta noAWS Management Console.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Política gerenciada da AWS: AWSAccountManagementFullAccess

É possível anexar a política `AWSAccountManagementFullAccess` a suas identidades do IAM.

Essa política fornece acesso administrativo total para visualizar ou modificar o seguinte:

- Os metadados sobre seuContas da AWS
- ORegiões da AWSque estão habilitados ou desativados para oConta da AWS(você pode ver o status ou ativar ou desativar regiões para sua conta somente usando oAWSconsole)

Ele faz isso concedendo permissão para executar qualquer`account`operações.

Detalhes da permissão

Esta política inclui as seguintes permissões.

- `account`— Permite que os diretores visualizem ou modifiquem as informações de metadados sobreContas da AWS. Também permite que os diretores listem oRegiões da AWSque estão habilitados para a conta e os ativam ou desativam noAWS Management Console.

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

```
    ]
}
```

Atualizações do gerenciamento de contas paraAWSpolíticas gerenciadas

Exibir detalhes sobre as atualizações doAWSgerenciou políticas para gerenciamento de contas desde que esse serviço começou a rastrear essas mudanças. Para alertas automáticos sobre alterações nesta página, assine o feed RSS na página de histórico de documentos de gerenciamento de contas.

Alteração	Descrição	Data
AWSO gerenciamento de contas foi lançado com o novoAWSgerenciei políticas e comecei a monitorar as mudanças	O gerenciamento de contas foi lançado inicialmente com o seguinteAWSpolíticas gerenciadas: • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	30 de setembro de 2021

Validação de conformidade para gerenciamento de AWS contas

Auditores terceirizados avaliam a segurança e a conformidade dos AWS serviços que podem ser executados em você Conta da AWS como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte Serviços da AWSescopo por programa de conformidade Serviços da AWS . Para obter informações gerais, consulte Programas de conformidade da AWS.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Como AWS Artifact baixar relatórios em no Guia do AWS Artifact usuário.

Sua responsabilidade de conformidade ao usar serviços em sua empresa Conta da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa

e pelas leis e regulamentações aplicáveis. AWSfornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido de segurança e conformidade: estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services): esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

> **Note**
>
> Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- Recursos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Avaliar recursos com regras no AWS Config Developer Guide (Guia do desenvolvedor do CCI): o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: esse Serviço da AWS fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a conferir sua conformidade com padrões e práticas recomendadas de segurança do setor.
- AWS Audit Manager: esse Serviço da AWS ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência noAWSGerenciamento de contas

OAWSA infraestrutura global da é criada com baseRegiões da AWSe zonas de disponibilidade. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, altas taxas de transferência e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

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

Segurança da infraestrutura no AWS Account Management

Como serviços gerenciados, AWS os serviços executados em você Conta da AWS são protegidos pela segurança de rede AWS global. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar as configurações da conta 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 perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Monitorando o gerenciamento de AWS contas

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho do gerenciamento de AWS contas e de suas outras AWS soluções. AWSfornece as seguintes ferramentas de monitoramento para monitorar o gerenciamento de contas, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- AWS CloudTrailcaptura (registra) chamadas de API e eventos relacionados feitos por você ou em seu nome Conta da AWS e grava os arquivos de log em um bucket do Amazon Simple Storage Service (Amazon S3) especificado por você. Isso permite identificar quais usuários e contas ligaramAWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.
- EventBridgeA Amazon adiciona automação adicional aos seus AWS serviços ao responder automaticamente aos eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

Registro em logAWSUsando as chamadas à API de gerenciamento de contasAWS CloudTrail

OAWSAs APIs de gerenciamento de contas são integradas comAWS CloudTrail, um serviço que fornece um registro das ações executadas por um usuário, uma função ou umaAWSserviço que chama uma operação de Gerenciamento de Conta. O CloudTrail captura todas as chamadas de API de Gerenciamento de contas como eventos. As chamadas capturadas incluem todas as chamadas para as operações de Gerenciamento de Conta. Se você criar uma trilha, será possível ativar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para operações de gerenciamento de contas. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação que chamou uma operação de Gerenciamento de conta, o endereço IP usado para fazer a solicitação, quem fez a solicitação e quando, além de detalhes adicionais.

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

Informações de gerenciamento de contas no CloudTrail

O CloudTrail está habilitado noConta da AWSQuando você cria a conta. Quando ocorre uma atividade com uma operação de Gerenciamento de conta, o CloudTrail registra essa atividade em um evento do CloudTrail junto com outrosAWSEventos de serviço emHistórico de eventos. Você pode visualizar, pesquisar e fazer download de eventos recentes em suaConta da AWS. Para mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos em suaConta da AWS, incluindo eventos para operações de Gerenciamento de contas, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha naAWS Management Console, a trilha se aplica a todosRegiões 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. É possível configurar outros serviços da AWS para analisar e atuar mais profundamente sobre os dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Recebimento de arquivos de log do CloudTrail de várias regiões
- Recebimento de arquivos de log do CloudTrail de várias contas

AWS CloudTrailregistra todas as operações da API de gerenciamento de contas encontradas naReferência de API doSeção deste guia. Por exemplo, as chamadas para as operações `CreateAccount`, `DeleteAlternateContact` e `PutAlternateContact` geram entradas nos arquivos de log do CloudTrail.

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 o usuário raiz ouAWS Identity and Access ManagementCredenciais de usuário (IAM)
- Se a solicitação tiver sido feita com credenciais de segurança temporárias de uma função do IAM ou de um usuário federado
- Se a solicitação foi feita por outro serviço da AWS

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre as entradas de registro do Gerenciamento

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a operação solicitada, a data e a hora da operação, os parâmetros de solicitação etc. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Exemplo 1: O exemplo a seguir mostra uma entrada de log do CloudTrail para uma chamada do`GetAlternateContact`operação para recuperar a corrente`OPERATIONS`contato alternativo para uma conta. Os valores retornados pela operação não estão incluídos nas informações registradas.

Example Exemplo 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
```

```
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Exemplo 2: O exemplo a seguir mostra uma entrada de log do CloudTrail para uma chamada do`PutAlternateContact`Para adicionar uma nova`BILLING`contato alternativo para uma conta.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
```

```
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Exemplo 3: O exemplo a seguir mostra uma entrada de log do CloudTrail para uma chamada do`DeleteAlternateContact`Para excluir o atual`OPERATIONS`Contato alternativo.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
```

```
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Monitorando eventos de gerenciamento de contas com EventBridge

A Amazon EventBridge, anteriormente chamada de CloudWatch Eventos, ajuda você a monitorar eventos específicos e iniciar ações-alvo que usam outros. Serviços da AWS Os eventos de Serviços da AWS são entregues quase EventBridge em tempo real.

Usando EventBridge, você pode criar regras que correspondam aos eventos recebidos e encaminhá-los aos alvos para processamento.

Para obter mais informações, consulte Introdução à Amazon EventBridge no Guia do EventBridge usuário da Amazon.

Eventos de gerenciamento de contas

Os exemplos a seguir mostram eventos para gerenciamento de contas. Os eventos são emitidos com base no melhor esforço.

No momento, somente eventos específicos para ativar e desativar regiões e chamadas de API CloudTrail estão disponíveis para o gerenciamento de contas.

Event types (Tipos de evento)

- Evento para ativar e desativar regiões

Evento para ativar e desativar regiões

Quando você ativa ou desativa uma região em uma conta, seja no console ou na API, uma tarefa assíncrona é iniciada. A solicitação inicial será registrada como um CloudTrail evento na conta de destino. Além disso, um EventBridge evento será enviado para a conta de chamada quando o processo de ativação ou desativação for iniciado e novamente quando o processo for concluído.

O exemplo de evento a seguir mostra como uma solicitação será enviada indicando que `2020-09-30` a `ap-east-1` região era `ENABLED` por conta`123456789012`.

```
{
   "version":"0",
   "id":"11112222-3333-4444-5555-666677778888",
   "detail-type":"Region Opt-In Status Change",
   "source":"aws.account",
   "account":"123456789012",
   "time":"2020-09-30T06:51:08Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:account::123456789012:account"
   ],
   "detail":{
      "accountId":"123456789012",
      "regionName":"ap-east-1",
      "status":"ENABLED"
   }
}
```

Há quatro status possíveis que correspondem aos status retornados pelas APIs `GetRegionOptStatus` e`ListRegions`:

- `ENABLED`— A região foi habilitada com sucesso para o `accountId` indicado
- `ENABLING`— A região está em processo de habilitação para o `accountId` indicado
- `DISABLED`— A região foi desativada com sucesso para o `accountId` indicado

- `DISABLING`— A Região está em processo de desativação para o `accountId` indicado

O exemplo de padrão de evento a seguir cria uma regra que captura todos os eventos da região.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ]
}
```

O exemplo de padrão de evento a seguir cria uma regra que captura somente eventos `ENABLED` de uma `DISABLED` região.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ],
   "detail":{
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

Referência da API

As operações da API no Gerenciamento de Contas (`account`) O namespace permite que você modifique seuConta da AWS.

CadaConta da AWSsuporta metadados com informações sobre a conta, incluindo informações sobre até três contatos alternativos associados à conta. Eles são adicionais ao endereço de e-mail associado aousuário rootda conta. Você pode especificar somente um de cada um dos seguintes tipos de contato associados a uma conta.

- Contato de cobrança
- Contato de operações
- Contato de segurança

Por padrão, as operações de API discutidas neste guia se aplicam diretamente à conta que chama a operação. Oidentificaçãona conta que está chamando a operação, normalmente há uma função do IAM ou um usuário do IAM e deve ter permissão aplicada por uma política do IAM para chamar a operação da API. Como alternativa, você pode chamar essas operações de API a partir de uma identidade em umAWS Organizationsconta de gerenciamento e especifique o número de ID da conta para qualquerConta da AWSque é membro da organização.

Versão da API

Esta versão da Referência da API de Contas documenta a versão 2021-02-01 da API de gerenciamento de contas.

> **Note**
>
> Como alternativa ao uso direto da API, você pode usar um dosAWSSDKs, que consistem em bibliotecas e código de amostra para várias linguagens e plataformas de programação (Java, Ruby, .NET, iOS, Android e muito mais). Os SDKs fornecem uma maneira conveniente de criar acesso programático aoAWSOrganizações. Por exemplo, os SDKs cuidam da assinatura criptográfica de solicitações, do gerenciamento de erros e da repetição automática de solicitações. Para obter mais informações sobre os SDKs da AWS, incluindo como fazer download deles e instalá-los, consulte Ferramentas da Amazon Web Services.

Recomendamos que você use oAWSSDKs para fazer chamadas programáticas de API para o serviço de gerenciamento de contas. No entanto, você também pode usar a API de consulta de gerenciamento de contas para fazer chamadas diretas para o serviço web de gerenciamento de contas. Para saber mais sobre a API de consulta de gerenciamento de contas, consulteChamar a API por meio de solicitações de consulta HTTPno Guia do usuário de gerenciamento de contas. As organizações oferecem suporte às solicitações GET e POST para todas as ações. Ou seja, a API não exige que você use GET para algumas ações e POST para outras. No entanto, as solicitações GET estão sujeitas à limitação do tamanho de um URL. Portanto, para operações que exigem tamanhos maiores, use uma solicitação POST.

Assinatura de solicitações

Quando você envia solicitações HTTP paraAWS, você deve assinar as solicitações para queAWSpode identificar quem os enviou. Você assina solicitações com seuAWSchave de acesso, que consiste em um ID de chave de acesso e uma chave de acesso secreta. É altamente recomendável que você não crie uma chave de acesso para sua conta root. Qualquer pessoa que tenha a chave de acesso da sua conta root tem acesso irrestrito a todos os recursos da sua conta. Em vez disso, crie uma chave de acesso para um usuário do IAM que tenha privilégios administrativos. Como outra opção, useAWSServiço de Token de Segurança para gerar credenciais de segurança temporárias e usar essas credenciais para assinar solicitações.

Para assinar solicitações, recomendamos que você use o Signature Version 4. Se você tiver um aplicativo existente que usa o Signature Version 2, não precisa atualizá-lo para usar o Signature Version 4. No entanto, algumas operações agora exigem o Signature Version 4. A documentação das operações que exigem a versão 4 indica esse requisito. Para obter mais informações, consulte Assinar solicitações de API da AWS no Guia do usuário do IAM.

Quando você usa oAWSInterface de linha de comando (AWSCLI) ou um dosAWSSDKs para fazer solicitações paraAWS, essas ferramentas assinam automaticamente as solicitações para você com a chave de acesso que você especifica ao configurar as ferramentas.

Suporte e feedback para gerenciamento de contas

Os seus comentários são bem-vindos. Envie seus comentários parafeedback-awsaccounts@amazon.comou publique seus comentários e perguntas noFórum de suporte ao gerenciamento de contas. Para obter mais informações sobre os fóruns de suporte da AWS, consulte Ajuda com os fóruns.

Como os exemplos são apresentados

O JSON retornado pelo Gerenciamento de Contas como resposta às suas solicitações é retornado como uma única sequência longa sem quebras de linha ou espaços em branco de formatação. Tanto as quebras de linha quanto os espaços em branco são mostrados nos exemplos deste guia para melhorar a legibilidade. Quando exemplos de parâmetros de entrada também resultariam em sequências longas que se estenderiam além da tela, inserimos quebras de linha para melhorar a legibilidade. Você sempre deve enviar a entrada como uma única string de texto JSON.

Gravando solicitações de API

Suporte ao gerenciamento de contasCloudTrail, um serviço que registraAWSChamadas de API para seuConta da AWSe entrega arquivos de log para um bucket do Amazon S3. Usando informações coletadas porCloudTrail, você pode determinar quais solicitações foram feitas com êxito ao Gerenciamento de Contas, quem fez a solicitação, quando ela foi feita e assim por diante. Para saber mais sobre o gerenciamento de contas e seu suporte paraCloudTrail, vejaRegistro em logAWSUsando as chamadas à API de gerenciamento de contasAWS CloudTrail. Para saber mais sobreCloudTrail, incluindo como ativá-lo e encontrar seus arquivos de log, consulte oAWS CloudTrailGuia do usuário.

Ações

As ações a seguir são compatíveis:

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAlternateContact
- PutContactInformation
- StartPrimaryEmailUpdate

AcceptPrimaryEmailUpdate

Aceita a solicitação originada StartPrimaryEmailUpdate para atualizar o endereço de e-mail principal (também conhecido como endereço de e-mail do usuário raiz) da conta especificada.

Sintaxe da Solicitação

```
POST /acceptPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "Otp": "string",
   "PrimaryEmail": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

Essa operação só pode ser chamada da conta de gerenciamento ou da conta de administrador delegado de uma organização para uma conta de membro.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`.

Tipo: string

Padrão: `^\d{12}$`

Exigido: Sim

Otp

O código OTP enviado para o `PrimaryEmail` especificado na chamada da `StartPrimaryEmailUpdate` API.

Tipo: string

Padrão: `^[a-zA-Z0-9]{6}$`

Exigido: Sim

PrimaryEmail

O novo endereço de e-mail principal para uso com a conta especificada. Isso deve corresponder ao `PrimaryEmail` da chamada `StartPrimaryEmailUpdate` da API.

Tipo: string

Restrições de comprimento: comprimento mínimo de 5. Comprimento máximo de 64.

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "Status": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Status

Recupera o status da solicitação de atualização de e-mail principal aceita.

Tipo: sequências

Valores Válidos: `PENDING | ACCEPTED`

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

ConflictException

A solicitação não pôde ser processada devido a um conflito no status atual do recurso. Por exemplo, isso acontece se você tentar habilitar uma região que está sendo desativada no momento (no status DESABILITANDO) ou se você tentar alterar o e-mail do usuário raiz de uma conta para um endereço de e-mail que já está em uso.

Código de Status HTTP: 409

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

A operação falhou porque especificou um recurso que não pode ser encontrado.

Código de Status HTTP: 404

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteAlternateContact

Exclui o contato alternativo especificado de um Conta da AWS.

Para obter detalhes completos sobre como usar as operações de contato alternativo, consulte Acessar ou atualizar os contatos alternativos.

> **Note**
>
> Antes de atualizar as informações de contato alternativas de uma Conta da AWS que é gerenciada por AWS Organizations, você deve primeiro habilitar a integração entre AWS Account Management e Organizations. Para obter mais informações, consulte Habilitando o acesso confiável para o gerenciamento de AWS contas.

Sintaxe da Solicitação

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos da AWS conta que você deseja acessar ou modificar com essa operação.

Se você não especificar esse parâmetro, o padrão será a AWS conta da identidade usada para chamar a operação.

Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado, e a ID da conta especificada deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`; ela deve chamar a operação em um contexto independente sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro e chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: não

AlternateContactType

Especifica quais contatos alternativos devem ser excluídos.

Tipo: strings

Valores Válidos: `BILLING | OPERATIONS | SECURITY`

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 200 com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

A operação falhou porque especificou um recurso que não pode ser encontrado.

Código de Status HTTP: 404

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Exemplos

Exemplo 1

O exemplo a seguir exclui o contato alternativo de segurança da conta cujas credenciais são usadas para chamar a operação.

Exemplo de solicitação

```
POST / HTTP/1.1
```

```
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Resposta da amostra

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Exemplo 2

O exemplo a seguir exclui o contato alternativo de cobrança da conta membro especificada em uma organização. Você deve usar as credenciais da conta de gerenciamento da organização ou da conta de administrador delegado do serviço de gerenciamento de contas.

Exemplo de solicitação

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "BILLING" }
```

Resposta da amostra

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DisableRegion

Desativa (exclui) uma região específica para uma conta.

> **Note**
>
> O ato de desativar uma região removerá todo o acesso do IAM a quaisquer recursos que residam nessa região.

Sintaxe da Solicitação

```
POST /disableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Se você não especificar esse parâmetro, o padrão é a conta da Amazon Web Services da identidade usada para chamar a operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`. Ele deve chamar a operação em um contexto autônomo sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro. Em vez disso, chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: Não

RegionName

Especifica o código de região para um determinado nome de região (por exemplo,). `af-south-1` Quando você desativa uma região, AWS executa ações para desativar essa região em sua conta, como destruir recursos do IAM na região. Esse processo leva alguns minutos para a maioria das contas, mas poderá levar algumas horas. Você não pode ativar a Região até que o processo de desativação seja totalmente concluído.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Tamanho máximo de 50.

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

ConflictException

A solicitação não pôde ser processada devido a um conflito no status atual do recurso. Por exemplo, isso acontece se você tentar habilitar uma região que está sendo desativada no momento (no status DESABILITANDO) ou se você tentar alterar o e-mail do usuário raiz de uma conta para um endereço de e-mail que já está em uso.

Código de Status HTTP: 409

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface

- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

EnableRegion

Ativa (aceita) uma região específica para uma conta.

Sintaxe da Solicitação

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Se você não especificar esse parâmetro, o padrão é a conta da Amazon Web Services da identidade usada para chamar a operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`. Ele deve chamar a operação em um contexto autônomo sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro. Em vez disso, chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: Não

RegionName

Especifica o código de região para um determinado nome de região (por exemplo,). `af-south-1` Quando você habilita uma região, a AWS executa ações para preparar sua conta nesta região, como a distribuição dos seus recursos do IAM para a região. Esse processo leva alguns minutos para a maioria das contas, mas pode levar várias horas. Você não pode usar a região até que esse processo seja concluído. Além disso, você não pode desativar a Região até que o processo de habilitação seja totalmente concluído.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Tamanho máximo de 50.

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

ConflictException

A solicitação não pôde ser processada devido a um conflito no status atual do recurso. Por exemplo, isso acontece se você tentar habilitar uma região que está sendo desativada no momento (no status DESABILITANDO) ou se você tentar alterar o e-mail do usuário raiz de uma conta para um endereço de e-mail que já está em uso.

Código de Status HTTP: 409

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

GetAlternateContact

Recupera o contato alternativo especificado anexado a um Conta da AWS.

Para obter detalhes completos sobre como usar as operações de contato alternativo, consulte Acessar ou atualizar os contatos alternativos.

> **Note**
>
> Antes de atualizar as informações de contato alternativas de uma Conta da AWS que é gerenciada por AWS Organizations, você deve primeiro habilitar a integração entre AWS Account Management e Organizations. Para obter mais informações, consulte Habilitando o acesso confiável para o gerenciamento de AWS contas.

Sintaxe da Solicitação

```
POST /getAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos da AWS conta que você deseja acessar ou modificar com essa operação.

Se você não especificar esse parâmetro, o padrão será a AWS conta da identidade usada para chamar a operação.

Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado, e a ID da conta especificada deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`; ela deve chamar a operação em um contexto independente sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro e chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: não

AlternateContactType

Especifica qual contato alternativo você deseja recuperar.

Tipo: strings

Valores Válidos: `BILLING | OPERATIONS | SECURITY`

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AlternateContact": {
      "AlternateContactType": "string",
      "EmailAddress": "string",
      "Name": "string",
```

```
        "PhoneNumber": "string",
        "Title": "string"
    }
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AlternateContact

Uma estrutura que contém os detalhes do contato alternativo especificado.

Tipo: objeto AlternateContact

Erros

Para obter informações sobre os erros comuns a todas as ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

A operação falhou porque especificou um recurso que não pode ser encontrado.

Código de Status HTTP: 404

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Exemplos

Exemplo 1

O exemplo a seguir recupera o contato alternativo de segurança da conta cujas credenciais são usadas para chamar a operação.

Exemplo de solicitação

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Resposta da amostra

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Security"
    }
}
```

Exemplo 2

O exemplo a seguir recupera o contato alternativo de operações para a conta membro especificada em uma organização. Você deve usar as credenciais da conta de gerenciamento da organização ou da conta de administrador delegado do serviço de gerenciamento de contas.

Exemplo de solicitação

```
POST / HTTP/1.1
```

```
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "Operations" }
```

Resposta da amostra

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Operations"
    }
}
```

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetContactInformation

Recupera as principais informações de contato de um Conta da AWS.

Para obter detalhes completos sobre como usar as operações de contato principal, consulte Atualizar as informações de contato principal e alternativo.

Sintaxe da Solicitação

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Se você não especificar esse parâmetro, o padrão é a conta da Amazon Web Services da identidade usada para chamar a operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`. Ele deve chamar a operação em um contexto autônomo sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro. Em vez disso, chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

ContactInformation

Contém os detalhes das principais informações de contato associadas a um Conta da AWS.

Tipo: objeto ContactInformation

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

A operação falhou porque especificou um recurso que não pode ser encontrado.

Código de Status HTTP: 404

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetPrimaryEmail

Recupera o endereço de e-mail principal da conta especificada.

Sintaxe da Solicitação

```
POST /getPrimaryEmail HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

Essa operação só pode ser chamada da conta de gerenciamento ou da conta de administrador delegado de uma organização para uma conta de membro.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`.

Tipo: string

Padrão: ^\d{12}$

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "PrimaryEmail": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

PrimaryEmail

Recupera o endereço de e-mail principal associado à conta especificada.

Tipo: string

Restrições de comprimento: comprimento mínimo de 5. Comprimento máximo de 64.

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

A operação falhou porque especificou um recurso que não pode ser encontrado.

Código de Status HTTP: 404

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetRegionOptStatus

Recupera o status de aceitação de uma região específica.

Sintaxe da Solicitação

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Se você não especificar esse parâmetro, o padrão é a conta da Amazon Web Services da identidade usada para chamar a operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`. Ele deve chamar a operação em um contexto autônomo sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro. Em vez disso, chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: Não

RegionName

Especifica o código de região para um determinado nome de região (por exemplo,). `af-south-1` Essa função retornará o status de qualquer região que você passar para esse parâmetro.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Tamanho máximo de 50.

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "RegionName": "string",
   "RegionOptStatus": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

RegionName

O código da região que foi passado.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Tamanho máximo de 50.

RegionOptStatus

Um dos possíveis status que uma região pode ter (Ativado, Ativado, Desativado, Desativado, Ativado_By_Default).

Tipo: sequências

Valores Válidos: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRegions

Lista todas as regiões de uma determinada conta e seus respectivos status de aceitação. Opcionalmente, essa lista pode ser filtrada pelo `region-opt-status-contains` parâmetro.

Sintaxe da Solicitação

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "MaxResults": number,
   "NextToken": "string",
   "RegionOptStatusContains": [ "string" ]
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Se você não especificar esse parâmetro, o padrão é a conta da Amazon Web Services da identidade usada para chamar a operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`. Ele deve chamar a operação em um contexto autônomo sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro. Em vez disso, chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: Não

MaxResults

O número total de itens a serem retornados na saída do comando. Se o número total de itens disponíveis for maior que o valor especificado, a `NextToken` será fornecido na saída do comando. Para retomar a paginação, forneça o valor `NextToken` no argumento `starting-token` de um comando subsequente. Não use o elemento de `NextToken` resposta diretamente fora da AWS CLI. Para exemplos de uso, consulte Paginação no Guia do usuário da interface de linha de AWS comando.

Tipo: número inteiro

Faixa válida: valor mínimo de 1. Valor máximo de 50.

Obrigatório: Não

NextToken

Um token usado para especificar por onde começar a paginar. Isso é `NextToken` de uma resposta previamente truncada. Para exemplos de uso, consulte Paginação no Guia do usuário da interface de linha de AWS comando.

Tipo: string

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 1.000.

Obrigatório: Não

RegionOptStatusContains

Uma lista de status de região (Ativado, Ativado, Desativado, Desativado, Ativado_por_padrão) a serem usados para filtrar a lista de regiões de uma determinada conta. Por exemplo, passar um valor de ENABLING só retornará uma lista de regiões com o status de Região ENABLING.

Tipo: Matriz de strings

Valores Válidos: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Obrigatório: Não

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Regions": [
      {
         "RegionName": "string",
         "RegionOptStatus": "string"
      }
   ]
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

NextToken

Se houver mais dados a serem retornados, eles serão preenchidos. Ele deve ser passado para o parâmetro de `next-token` solicitação de`list-regions`.

Tipo: string

Regions

Essa é uma lista de regiões para uma determinada conta ou, se o parâmetro filtrado foi usado, uma lista de regiões que correspondem aos critérios de filtro definidos no `filter` parâmetro.

Tipo: matriz de objetos Region

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

PutAlternateContact

Modifica o contato alternativo especificado anexado a um Conta da AWS.

Para obter detalhes completos sobre como usar as operações de contato alternativo, consulte Acessar ou atualizar os contatos alternativos.

> **Note**
>
> Antes de atualizar as informações de contato alternativas de uma Conta da AWS que é gerenciada por AWS Organizations, você deve primeiro habilitar a integração entre AWS Account Management e Organizations. Para obter mais informações, consulte Habilitando o acesso confiável para o gerenciamento de AWS contas.

Sintaxe da Solicitação

```
POST /putAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string",
   "EmailAddress": "string",
   "Name": "string",
   "PhoneNumber": "string",
   "Title": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos que você deseja acessar ou modificar com essa operação. AWS

Se você não especificar esse parâmetro, o padrão será a AWS conta da identidade usada para chamar a operação.

Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado, e a ID da conta especificada deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`; ela deve chamar a operação em um contexto independente sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro e chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: Não

AlternateContactType

Especifica qual contato alternativo você deseja criar ou atualizar.

Tipo: sequências

Valores Válidos: `BILLING | OPERATIONS | SECURITY`

Obrigatório: Sim

EmailAddress

Especifica um endereço de e-mail para o contato alternativo.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 254.

Padrão: `^[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*$`

Exigido: Sim

Name

Especifica um nome para o contato alternativo.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 64.

Obrigatório: Sim

PhoneNumber

Especifica um número de telefone para o contato alternativo.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 25.

Padrão: `^[\s0-9()+-]+$`

Exigido: Sim

Title

Especifica um título para o contato alternativo.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Tamanho máximo de 50.

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Exemplos

Exemplo 1

O exemplo a seguir define o contato alternativo de cobrança da conta cujas credenciais são usadas para chamar a operação.

Exemplo de solicitação

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
```

```
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Resposta da amostra

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Exemplo 2

O exemplo a seguir define ou substitui o contato alternativo de cobrança da conta membro especificada em uma organização. Você deve usar as credenciais da conta de gerenciamento da organização ou da conta de administrador delegado do serviço de gerenciamento de contas.

Exemplo de solicitação

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AccountId": "123456789012",
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Resposta da amostra

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface

- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

PutContactInformation

Atualiza as informações de contato primárias de um Conta da AWS.

Para obter detalhes completos sobre como usar as operações de contato principal, consulte Atualizar as informações de contato principal e alternativo.

Sintaxe da Solicitação

```
POST /putContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Se você não especificar esse parâmetro, o padrão é a

conta da Amazon Web Services da identidade usada para chamar a operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`. Ele deve chamar a operação em um contexto independente sem incluir o `AccountId` parâmetro.

Para chamar essa operação em uma conta que não é membro de uma organização, não especifique esse parâmetro. Em vez disso, chame a operação usando uma identidade pertencente à conta cujos contatos você deseja recuperar ou modificar.

Tipo: string

Padrão: `^\d{12}$`

Obrigatório: Não

ContactInformation

Contém os detalhes das principais informações de contato associadas a um Conta da AWS.

Tipo: objeto ContactInformation

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

StartPrimaryEmailUpdate

Inicia o processo de atualização do endereço de e-mail principal da conta especificada.

Sintaxe da Solicitação

```
POST /startPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "PrimaryEmail": "string"
}
```

Parâmetros da solicitação de URI

A solicitação não usa nenhum parâmetro de URI.

Corpo da Solicitação

A solicitação aceita os dados a seguir no formato JSON.

AccountId

Especifica o número de identificação da conta de 12 dígitos Conta da AWS que você deseja acessar ou modificar com essa operação. Para usar esse parâmetro, o chamador deve ser uma identidade na conta de gerenciamento da organização ou uma conta de administrador delegado. O ID da conta especificado deve ser uma conta membro na mesma organização. A organização deve ter todos os recursos habilitados e a organização deve ter acesso confiável habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta de administrador delegado atribuída.

Essa operação só pode ser chamada da conta de gerenciamento ou da conta de administrador delegado de uma organização para uma conta de membro.

> **Note**
>
> A conta de gerenciamento não pode especificar sua própria conta`AccountId`.

Tipo: string

Padrão: `^\d{12}$`

Exigido: Sim

PrimaryEmail

O novo endereço de e-mail principal (também conhecido como endereço de e-mail do usuário raiz) a ser usado na conta especificada.

Tipo: string

Restrições de comprimento: comprimento mínimo de 5. Comprimento máximo de 64.

Exigido: Sim

Sintaxe da Resposta

```
HTTP/1.1 200
Content-type: application/json

{
   "Status": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Status

O status da solicitação principal de atualização por e-mail.

Tipo: sequências

Valores Válidos: `PENDING | ACCEPTED`

Erros

Para obter informações sobre os erros comuns retornados pelas ações, consulte Erros comuns.

AccessDeniedException

A operação falhou porque a identidade de chamada não tem as permissões mínimas necessárias.

Código de Status HTTP: 403

ConflictException

A solicitação não pôde ser processada devido a um conflito no status atual do recurso. Por exemplo, isso acontece se você tentar habilitar uma região que está sendo desativada no momento (no status DESABILITANDO) ou se você tentar alterar o e-mail do usuário raiz de uma conta para um endereço de e-mail que já está em uso.

Código de Status HTTP: 409

InternalServerException

A operação falhou devido a um erro interno do AWS. Tente sua operação novamente mais tarde.

Código de Status HTTP: 500

ResourceNotFoundException

A operação falhou porque especificou um recurso que não pode ser encontrado.

Código de Status HTTP: 404

TooManyRequestsException

A operação falhou porque foi chamada com muita frequência e excedeu o limite do acelerador.

Código de Status HTTP: 429

ValidationException

A operação falhou porque um dos parâmetros de entrada era inválido.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS Command Line Interface
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

Ações relacionadas ao outroAWSserviços

As operações a seguir estão relacionadas aoAWS Account ManagementMas são parte doAWS OrganizationsNamespace:

- CreateAccount
- CreateGovCloudAccount
- DescribeAccount

CreateAccount

O`CreateAccount`A operação da API está disponível para uso somente no contexto de uma organização gerenciada peloAWS Organizationsserviço. A operação da API é definida no namespace desse serviço.

Para obter mais informações, consulteCreateAccountnoAWS OrganizationsReferência de API do.

CreateGovCloudAccount

O`CreateGovCloudAccount`A operação da API está disponível para uso somente no contexto de uma organização gerenciada peloAWS OrganizationsServiço. A operação da API é definida no namespace desse serviço.

Para obter mais informações, consulteCreateGovCloudAccountnoAWS OrganizationsReferência de API do.

DescribeAccount

O`DescribeAccount`A operação da API está disponível para uso somente no contexto de uma organização gerenciada peloAWS Organizationsserviço. A operação da API é definida no namespace desse serviço.

Para obter mais informações, consulteDescribeAccountnoAWS OrganizationsReferência de API do.

Tipos de dados

Os seguintes tipos de dados são compatíveis:

- AlternateContact
- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

Uma estrutura que contém os detalhes de um contato alternativo associado a uma AWS conta

Conteúdo

AlternateContactType

O tipo de contato alternativo.

Tipo: sequências

Valores Válidos: `BILLING | OPERATIONS | SECURITY`

Obrigatório: Não

EmailAddress

O endereço de e-mail associado a esse contato alternativo.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 254.

Padrão: `^[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*$`

Obrigatório: Não

Name

O nome associado a esse contato alternativo.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 64.

Obrigatório: Não

PhoneNumber

O número de telefone associado a esse contato alternativo.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 25.

Padrão: `^[\s0-9()+-]+$`

Obrigatório: Não

Title

O título associado a esse contato alternativo.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Tamanho máximo de 50.

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ContactInformation

Contém os detalhes das principais informações de contato associadas a um Conta da AWS.

Conteúdo

AddressLine1

A primeira linha do endereço de contato principal.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 60.

Obrigatório: Sim

City

A cidade do endereço de contato principal.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 50.

Obrigatório: Sim

CountryCode

O código de país de duas letras ISO-3166 para o endereço de contato principal.

Tipo: string

Restrições de comprimento: comprimento fixo de 2.

Obrigatório: Sim

FullName

O nome completo do endereço de contato principal.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 50.

Obrigatório: Sim

PhoneNumber

O número de telefone das informações de contato principais. O número será validado e, em alguns países, verificado para ativação.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 20.

Padrão: `^[+][\s0-9()-]+$`

Exigido: Sim

PostalCode

O código postal do endereço de contato principal.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 20.

Obrigatório: Sim

AddressLine2

A segunda linha do endereço de contato principal, se houver.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 60.

Obrigatório: não

AddressLine3

A terceira linha do endereço de contato principal, se houver.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 60.

Obrigatório: não

CompanyName

O nome da empresa associada às informações de contato primárias, se houver.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 50.

Obrigatório: não

DistrictOrCounty

O distrito ou condado do endereço de contato principal, se houver.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 50.

Obrigatório: não

StateOrRegion

O estado ou a região do endereço de contato principal. Se o endereço de correspondência estiver nos Estados Unidos (EUA), o valor nesse campo pode ser um código de estado de dois caracteres (por exemplo,`NJ`) ou o nome completo do estado (por exemplo,`New Jersey`). Esse campo é obrigatório nos seguintes países: `USCA`,`GB`,`DE`, `JPIN`,, `BR` e.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 50.

Obrigatório: não

WebsiteUrl

O URL do site associado às informações de contato primárias, se houver.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Obrigatório: não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK for C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Region

Essa é uma estrutura que expressa a região de uma determinada conta, consistindo em um nome e status de inscrição.

Conteúdo

RegionName

O código da região de uma determinada região (por exemplo,`us-east-1`).

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 50.

Obrigatório: não

RegionOptStatus

Um dos possíveis status que uma região pode ter (Ativado, Ativado, Desativado, Desativado, Ativado_By_Default).

Tipo: strings

Valores Válidos: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK for C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ValidationExceptionField

A entrada falhou em atender às restrições especificadas pelo AWS serviço em um campo especificado.

Conteúdo

message

Uma mensagem sobre a exceção de validação.

Tipo: string

Obrigatório: Sim

name

O nome do campo em que a entrada inválida foi detectada.

Tipo: string

Obrigatório: Sim

Consulte também

Para obter mais informações sobre como usar essa API em um dos AWS SDKs específicos da linguagem, consulte o seguinte:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Parâmetros gerais

A lista a seguir contém os parâmetros que todas as ações usam para assinar solicitações do Signature versão 4 com uma string de consulta. Todos os parâmetros específicos de uma ação são listados no tópico para a ação. Para obter mais informações sobre o Signature versão 4, consulte Solicitações deAWS API de assinatura no Guia do usuário do IAM.

Action

A ação a ser executada.

Tipo: string

Obrigatório: sim

Version

A versão da API para a qual a solicitação foi escrita, expressa no formato AAAA-MM-DD.

Tipo: string

Obrigatório: sim

X-Amz-Algorithm

O algoritmo de hash que foi usado para criar a assinatura da solicitação.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Valores válidos: `AWS4-HMAC-SHA256`

Obrigatório: Condicional

X-Amz-Credential

O valor de escopo da credencial, uma string que inclui a sua chave de acesso, a data, a região visada, o serviço que está sendo solicitado e uma sequência de encerramento ("aws4_request"). O valor é expresso no seguinte formato: chave_acesso/AAAAMMDD/região/serviço/aws4_request.

Para obter mais informações, consulte Criar uma solicitação deAWS API assinada no Guia do usuário do IAM.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

X-Amz-Date

A data usada para criar a assinatura. O formato deve ser o formato básico ISO 8601 (AAAAMMDD'T'HHMMSS'Z'). Por exemplo, a data/hora a seguir é um valor X-Amz-Date válido: `20120325T120000Z`.

Condição: X-Amz-Date é opcional para todas as solicitações e pode ser usado para substituir a data usada para assinar solicitações. Se o cabeçalho Date (Data) for especificado no formato básico ISO 8601, o valor X-Amz-Date não será necessário. Quando X-Amz-Date é usado, sempre substitui o valor do cabeçalho Date (Data). Para obter mais informações, consulte Elementos de uma assinatura de solicitação deAWS API no Guia do usuário do IAM.

Tipo: string

Obrigatório: Condicional

X-Amz-Security-Token

O token de segurança temporário que foi obtido por meio de uma chamada paraAWS Security Token Service (AWS STS). Para obter uma lista de serviços que são compatíveis com credenciais de segurança temporárias doAWS STS, vá para Serviços da AWSque funcionam com o IAM no Manual do usuário do IAM.

Condição: se estiver usando credenciais de segurança temporárias doAWS STS, você deverá incluir o token de segurança.

Tipo: string

Obrigatório: Condicional

X-Amz-Signature

Especifica a assinatura com codificação hexadecimal que foi calculada com base na string a ser assinada e na chave de assinatura derivada.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

X-Amz-SignedHeaders

Especifica todos os cabeçalhos HTTP que foram incluídos como parte da solicitação canônica. Para obter mais informações sobre como especificar cabeçalhos assinados, consulte Criar uma solicitação deAWS API assinada no Guia do usuário do IAM.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

Erros comuns

Esta seção lista os erros comuns às ações de API de todos os serviços da AWS. Para saber os erros específicos de uma ação de API para esse serviço, consulte o tópico sobre a ação de API em questão.

AccessDeniedException

Você não tem acesso suficiente para executar essa ação.

Código de status HTTP: 400

IncompleteSignature

A assinatura da solicitação não segue os padrões da AWS.

Código de status HTTP: 400

InternalFailure

O processamento da solicitação falhou por causa de um erro, uma exceção ou uma falha desconhecida.

Código de status HTTP: 500

InvalidAction

A ação ou operação solicitada é inválida. Verifique se a ação foi digitada corretamente.

Código de status HTTP: 400

InvalidClientTokenId

O certificado X.509 ou o ID de chave de acesso da AWS fornecido não existe em nossos registros.

Código de status HTTP: 403

NotAuthorized

Você não tem permissão para realizar esta ação.

Código de status HTTP: 400

OptInRequired

O ID da chave de acesso da AWS precisa de uma assinatura do serviço.

Código de status HTTP: 403

RequestExpired

A solicitação atingiu o serviço mais de 15 minutos após a data na solicitação ou mais de 15 minutos após a data de expiração da solicitação (como para URLs predeterminados), ou a data na solicitação está a mais de 15 minutos no futuro.

Código de status HTTP: 400

ServiceUnavailable

Falha na solicitação devido a um erro temporário do servidor.

Código de status HTTP: 503

ThrottlingException

A solicitação foi negada devido à limitação da solicitação.

Código de status HTTP: 400

ValidationError

A entrada não atende às restrições especificadas por um serviço da AWS.

Código de status HTTP: 400

Chamar a API por meio de solicitações de consulta HTTP

Esta seção contém informações gerais sobre o uso da API de consulta paraAWSGerenciamento de contas. Para obter mais detalhes sobre as operações da API e os erros, consulte o Referência da API.

> **Note**
>
> Em vez de fazer chamadas diretas para oAWSAPI de consulta de gerenciamento de contas, você pode usar um dosAWSSDKs. Os SDKs da AWS consistem em bibliotecas e no código de exemplo para várias linguagens de programação e plataformas (Java, Ruby, .NET, iOS, Android e muito mais). Os SDKs fornecem uma maneira conveniente de criar acesso programático aoAWSGerenciamento de contas eAWS. Por exemplo, os SDKs processam tarefas como assinatura criptográfica de solicitações, gerenciamento de erros e novas tentativas automáticas de solicitações. Para obter informações sobre os AWS SDKs, incluindo como fazer download e instalá-los, consulte Ferramentas da Amazon Web Services.

Com a API de consulta paraAWSGerenciamento de contas, você pode chamar ações de serviço. As solicitações da API de consulta são solicitações HTTPS que devem conter um`Action`parâmetro para indicar a operação a ser executada.AWS Suportes de gerenciamento de contas`GET`e`POST`solicitações para todas as operações. Ou seja, a API não exige que você use`GET`para algumas ações e`POST`para outros. No entanto,`GET`as solicitações estão sujeitas ao tamanho limitado de um URL. Embora esse limite dependa do navegador, um limite típico é de 2.048 bytes. Portanto, para solicitações da API de consulta que exigem tamanhos maiores, você deve usar um`POST`pedido.

A resposta é um documento XML. Para obter mais detalhes sobre a resposta, consulte as páginas de ação individuais no Referência da API.

Tópicos

- Endpoints
- HTTPS obrigatório
- AssinaturaAWSSolicitações da API de gerenciamento de contas

Endpoints

AWSO gerenciamento de contas tem um único endpoint de API global hospedado no Leste dos EUA (Norte da Virgínia)Região da AWS.

Para obter mais informações sobre endpoints e regiões da AWS para todos os serviços, consulte Regiões e endpoints no Referência geral da AWS.

HTTPS obrigatório

Como a API Query pode retornar informações confidenciais, como credenciais de segurança, você deve usar HTTPS para criptografar todas as solicitações de API.

AssinaturaAWSSolicitações da API de gerenciamento de contas

As solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta. É altamente recomendável que você não use seuAWScredenciais da conta raiz para o trabalho diário comAWSGerenciamento de contas. Você pode usar as credenciais para umAWS Identity and Access ManagementCredenciais de usuário (IAM) ou temporárias, como as que você usa com uma função do IAM.

Para assinar suas solicitações de API, você deve usar a AWS Signature versão 4. Para obter informações sobre como usar o Signature versão 4, consulte Assinatura de solicitações de API da AWS no Guia do usuário do IAM.

Para obter mais informações, consulte as informações a seguir.

- Credenciais de segurança da AWS: fornece informações gerais sobre os tipos de credencial que você pode usar para acessar a AWS.
- Melhores práticas de segurança no IAM— Oferece sugestões para usar o serviço IAM para ajudar a proteger suaAWSrecursos, incluindo aqueles emAWSGerenciamento de contas.
- Credenciais de segurança temporárias no IAM: descreve como criar e usar credenciais de segurança temporárias.

Cotas para AWS Account Management

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. Salvo indicação em contrário, cada cota é específica Região da AWS.

Cada um Conta da AWS tem as seguintes cotas relacionadas ao gerenciamento de contas.

Recurso	Quota
Número máximo de `StartPrimaryEmailUpdate` solicitações por conta de destino	3 por 30 segundos
Número de contatos alternativos em um Conta da AWS	3 - um para cada `BILLINGSECURITY`, e `OPERATIONS`
Número de solicitações simultâneas de opção regional por conta	6
Número de solicitações simultâneas de opção regional por organização	20
Taxa de `AcceptPrimaryEmailUpdate` solicitações por conta de chamador	1 por segundo, dispare para 1 por segundo
Taxa de `DeleteAlternateContact` solicitações por conta	1 por segundo, dispare para 6 por segundo
Taxa de `DisableRegion` solicitações por conta	1 por segundo, dispare para 1 por segundo
Taxa de `EnableRegion` solicitações por conta	1 por segundo, dispare para 1 por segundo
Taxa de `GetAlternateContact` solicitações por conta	10 por segundo, dispare para 15 por segundo
Taxa de `GetContactInformation` solicitações por conta	10 por segundo, dispare para 15 por segundo

Recurso	Quota
Taxa de `GetPrimaryEmail` solicitações por conta de chamador	3 por segundo, dispare para 3 por segundo
Taxa de `GetRegionOptStatus` solicitações por conta	5 por segundo, dispare para 5 por segundo
Taxa de `ListRegions` solicitações por conta	5 por segundo, dispare para 5 por segundo
Taxa de `PutAlternateContact` solicitações por conta	5 por segundo, dispare para 8 por segundo
Taxa de `PutContactInformation` solicitações por conta	5 por segundo, dispare para 8 por segundo
Taxa de `StartPrimaryEmailUpdate` solicitações por conta de chamador	1 por segundo, dispare para 1 por segundo

Solução de problemas do seu Conta da AWS

Use as informações nos tópicos a seguir para ajudá-lo a diagnosticar e corrigir problemas com seuConta da AWS. Para obter ajuda com o usuário raiz, consulte Solução de problemas com o usuário raiz no Guia do usuário do IAM. Para obter ajuda com o processo de login, consulte Solução de problemas de Conta da AWS login no Guia do AWS usuário de login.

Tópicos de solução de problemas

- Solução de problemas com a Conta da AWS criação
- Solução de problemas com o Conta da AWS fechamento
- Solução de problemas com oContas da AWS

Solução de problemas com a Conta da AWS criação

Use os links de referência na tabela a seguir para ajudá-lo a diagnosticar e corrigir problemas com a criação de um novo Conta da AWS.

Problema	Link de referência	Origem
Não sei como me inscrever ou criar uma conta	Crie um autônomo Conta da AWS	Este guia
O que devo fazer se não receber uma ligação AWS para verificar minha nova conta ou se o PIN inserido não funcionar?	https://repost.aws/knowledge-center/ phone-verify-no-call	AWS re:Post
Como resolvo o erro “número máximo de tentativas malsucedidas” quando tento verificar minhas Conta da AWS por telefone?	https://repost.aws/knowledge-center/ maximum-failed-attempts	AWS re:Post

Problema	Link de referência	Origem
Já se passaram mais de 24 horas e minha conta não está ativada	https://repost.aws/knowledge-center/ create-and-activate-aws -conta	AWS re:Post
Não consigo entrar na minha nova conta depois que ela foi criada	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues .html	AWS Guia do usuário de login

Para obter ajuda adicional, recomendamos que você AWS re:Postpesquise conteúdo relacionado ao seu problema específico. Se você ainda precisar de ajuda, entre em contato AWS Support.

Solução de problemas com o Conta da AWS fechamento

Use as informações abaixo para ajudá-lo a diagnosticar e corrigir problemas comuns encontrados durante o processo de encerramento da conta. Para obter informações gerais sobre o processo de encerramento da conta, consulteFechar um Conta da AWS.

Tópicos

Não sei como excluir ou cancelar minha conta

Para fechar sua conta, siga as instruções emFechar um Conta da AWS.

Não vejo o botão Fechar conta na página Contas

Se você não estiver conectado como usuário root, não verá o botão Fechar conta exibido na página Contas. Você deve fazer login no AWS Management Console como usuário root para fechar sua conta. Se você não conseguir fazer login, consulte Solução de problemas com o usuário root.

Fechei minha conta, mas ainda não recebi um e-mail de confirmação

Esse e-mail de confirmação é enviado somente para o endereço de e-mail do usuário raiz do Conta da AWS. Se você não receber esse e-mail em algumas horas, poderá fazer login no AWS Management Console como usuário root para verificar se sua conta foi encerrada. Se sua conta foi fechada com sucesso, você verá uma mensagem indicando que sua conta foi encerrada. Se a conta que você fechou for uma conta de membro, você poderá verificar se o encerramento foi bem-sucedido verificando se a conta fechada está marcada como `SUSPENDED` no AWS Organizations console. Para obter mais informações, consulte Fechar uma conta-membro na sua organização no Guia do usuário doAWS Organizations .

Se você estiver tentando fechar uma conta de gerenciamento e não receber um e-mail de confirmação sobre o encerramento da conta, sua organização provavelmente tem contas de membros ativas. Você só pode fechar a conta de gerenciamento se sua organização não tiver nenhuma conta de membro ativa. Para verificar se não há contas de membros ativas restantes em sua organização, acesse o AWS Organizations console e certifique-se de que todas as contas de membros estejam aparecendo ao `Suspended` lado dos nomes das contas. Depois disso, você pode fechar a conta de gerenciamento.

Eu recebo um erro ConstraintViolationException "" ao tentar fechar minha conta

Você está tentando fechar uma conta de gerenciamento usando o AWS Organizations console, o que não é possível. Para fechar uma conta de gerenciamento, você precisa fazer login AWS Management Console como usuário root da conta de gerenciamento e fechá-la na página Contas. Para obter mais informações, consulte Fechar uma conta de gerenciamento em sua organização no GuiaAWS Organizations do usuário.

Eu recebo um erro “CLOSE_ACCOUNT_QUOTA_EXCEEDED” ao tentar fechar uma conta de membro

Você só pode fechar 10% das contas dos membros em um período contínuo de 30 dias. Essa cota não está associada a um mês do calendário. A contagem começa assim que você encerra uma conta. Num prazo de 30 dias após o encerramento inicial da conta, você não poderá exceder o limite de 10% de encerramento da conta. O fechamento mínimo da conta é 10 e o fechamento máximo da conta é 1000, mesmo que 10% das contas excedam 1000. Para obter mais informações sobre cotas de Organizations, consulte Quotas para AWS Organizations no Guia do AWS Organizations Usuário.

Preciso excluir minha AWS organização antes de fechar a conta de gerenciamento?

Não, você não precisa excluir sua AWS organização antes de fechar a conta de gerenciamento. No entanto, você só pode fechar a conta de gerenciamento se sua organização não tiver nenhuma conta de membro ativa. Para verificar se não há contas de membros ativas restantes em sua organização, acesse o AWS Organizations console e certifique-se de que todas as contas de membros estejam aparecendo ao `Suspended` lado dos nomes das contas. Depois disso, você pode fechar a conta de gerenciamento.

Solução de problemas com oContas da AWS

Use estas informações para ajudá-lo a solucionar problemas relacionados aoConta da AWS.

Problemas

- Preciso alterar o cartão de crédito da minhaConta da AWS
- Preciso relatar fraudulentoConta da AWSatividade
- Preciso encerrar minhaConta da AWS

Preciso alterar o cartão de crédito da minhaConta da AWS

Para alterar o cartão de crédito doConta da AWS, você deve ser capazes de fazer login.AWSTem proteções que exigem que você prove que é o proprietário da conta da. Para obter instruções, consulteComo gerenciar as formas de pagamento de cartão de créditonoAWS BillingGuia do usuário do.

Preciso relatar fraudulentoConta da AWSatividade

Se você suspeitar de atividade fraudulenta usando seuConta da AWSe gostaria de fazer um relatório, vejaComo relato abuso deAWSrecursos.

Se você estiver tendo problemas com uma compra feita na Amazon.com, consulteAtendimento ao cliente da Amazon.

Preciso encerrar minhaConta da AWS

Para obter ajuda para solucionar problemas com o fechamento de seuConta da AWS, consulteFechar um Conta da AWS.

Histórico de documentos do Guia do usuário de gerenciamento de contas

A tabela a seguir descreve os lançamentos da documentação para gerenciamento de AWS contas.

Alteração	Descrição	Data
Novas APIs primárias de e-mail	Support for new`GetPrimaryEmail`,`StartPrimaryEmailUpdate`, and `AcceptPrimaryEmailUpdate` APIs para atualizar centralmente o endereço de e-mail do usuário raiz de qualquer conta de membro em. AWS Organizations Para obter mais informações, consulte Atualização do endereço de e-mail do usuário raiz para uma conta de membro no Guia AWS Organizations do usuário.	6 de junho de 2024
Reescrita do tópico de encerramento da conta	Reformulou completamente todo o tópico de encerramento de contas, incluindo a adição de etapas sobre como fechar contas de membros e de gerenciamento.	1 de fevereiro de 2024
Fim do suporte para adicionar novas perguntas sobre desafios de segurança	Novo conteúdo adicionado, observando que a opção de adicionar novas perguntas de desafio foi removida da página Contas.	5 de janeiro de 2024

Fim do suporte para o `aws-portal` namespace	AWS Identity and Access Management As ações (IAM) que eram usadas anteriormente para gerenciar sua conta (por exemplo, `aws-portal:ModifyAccount` e `aws-portal:ViewAccount`) chegaram ao fim do suporte padrão.	1º de janeiro de 2024
Reescrita do tópico Regiões	Reformulou completamente todo o tópico das Regiões, incluindo a adição de controles de expansão e retração.	8 de outubro de 2023
Tópicos do usuário raiz realocados para o Guia do usuário do IAM	Discussão consolidada sobre usuários raiz em um tópico, links de referência cruzada adicionados aos tópicos do usuário raiz que foram movidos para o Guia do usuário do IAM.	18 de setembro de 2023
Nova seção adicionada ao tópico de contato da conta principal	Foi adicionada uma nova seção de requisitos de número de telefone e endereço de e-mail.	12 de setembro de 2023
Novas APIs de informações de contato	Support para novas `PutContactInformation` APIs `GetContactInformation` e APIs.	22 de julho de 2022

AWS O gerenciamento de contas agora suporta a atualização de contatos alternativos por meio do AWS Organizations console.	Agora você pode atualizar os contatos alternativos da sua organização por meio do AWS Organizations console usando as permissões da API de conta fornecidas pelas políticas AWS Organizations gerenciadas atualizadas.	8 de fevereiro de 2022
Lançamento inicial	Versão inicial do Guia de referência de gerenciamento de AWS contas	30 de setembro de 2021

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

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.