



Guia de referência

# AWS Gerenciamento de contas



# AWS Gerenciamento de contas: Guia de referência

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

---

# Table of Contents

O que é um Conta da AWS? .....	1
Características de um Conta da AWS .....	3
Você é um AWS usuário iniciante? .....	3
AWS Serviços relacionados .....	4
Uso do usuário-raiz .....	5
Suporte e feedback .....	5
Outros AWS recursos .....	5
Conceitos básicos da conta .....	7
Revisar os pré-requisitos .....	7
Etapa 1: criar a conta .....	8
Etapa 2: ativar a MFA para o usuário-raiz .....	10
Etapa 3: criar um usuário administrador .....	11
Tópicos relacionados .....	11
Como acessar a conta .....	11
Planejar a estrutura de governança .....	13
Benefícios do uso de vários Contas da AWS .....	13
Gerenciando vários Contas da AWS .....	14
Quando usar AWS Organizations .....	15
Habilitar acesso confiável .....	16
Habilitar uma conta de administrador delegado .....	18
Restrinja o acesso usando SCPs .....	19
Quando usar AWS Control Tower .....	21
Noções básicas dos modos de operação da API .....	22
Conceder permissões para atualizar atributos da conta .....	23
Configurar a conta .....	26
Criar ou atualizar o alias da conta .....	26
Ativar ou desativar Regiões da AWS em sua conta .....	26
Referência de disponibilidade regional .....	29
Considerações antes de habilitar e desabilitar regiões .....	32
Tempos de processamento e limites de solicitação .....	33
Habilitar ou desabilitar região para contas autônomas .....	33
Habilitar ou desabilitar uma região na organização .....	36
Atualize o faturamento do seu Conta da AWS .....	38
Atualize o e-mail do usuário-raiz .....	38

Atualize o e-mail do usuário raiz (e-mail ) para uma conta autônoma Conta da AWS ou de gerenciamento .....	39
Atualize o e-mail do usuário raiz (e-mail ) para qualquer Conta da AWS pessoa em sua organização .....	41
Atualizar senha do usuário-raiz .....	44
Atualize seu Conta da AWS nome .....	45
Atualize o nome da sua conta para uma conta autônoma Conta da AWS .....	46
Atualize o nome da sua conta para qualquer Conta da AWS pessoa da sua organização .....	47
Atualize os contatos alternativos para o seu Conta da AWS .....	49
Requisitos de número de telefone e endereço de e-mail .....	50
Atualize os contatos alternativos para um autônomo Conta da AWS .....	50
Atualize os contatos alternativos de qualquer um Conta da AWS em sua organização .....	54
conta: chave de AlternateContactTypes contexto .....	57
Atualize o contato principal do seu Conta da AWS .....	58
Requisitos de número de telefone e endereço de e-mail .....	58
Atualizar o contato principal de uma conta autônoma Conta da AWS ou de gerenciamento .....	59
Atualize o contato principal de qualquer conta AWS membro em sua organização .....	61
Visualizar os identificadores da conta .....	64
Encontre seu Conta da AWS ID .....	65
Encontre o ID de usuário canônico para seu Conta da AWS .....	67
Proteger a conta .....	71
Proteção de dados .....	72
AWS PrivateLink .....	73
Criação do endpoint .....	73
Políticas de endpoint da Amazon VPC .....	74
Políticas de endpoint .....	74
Gerenciamento de Identidade e Acesso .....	75
Público .....	75
Autenticação com identidades .....	76
Gerenciar o acesso usando políticas .....	77
AWS Gerenciamento de contas e IAM .....	79
Exemplos de políticas baseadas em identidade .....	87
Usar políticas baseadas em identidade .....	90
Solução de problemas .....	93
AWS políticas gerenciadas .....	95

AWSAccountManagementReadOnlyAccess .....	96
AWSAccountManagementFullAccess .....	97
Atualizações da política .....	98
Validação de conformidade .....	98
Resiliência .....	99
Segurança da infraestrutura .....	100
Monitorar a conta .....	101
CloudTrail troncos .....	101
Informações de gerenciamento de contas em CloudTrail .....	102
Noções básicas das entradas de log do Gerenciamento de Contas .....	103
Monitorando eventos de gerenciamento de contas com EventBridge .....	106
Eventos do Gerenciamento de Contas .....	106
Solucionar problemas da conta .....	109
Problemas de criação da conta .....	109
Problemas com encerramento da conta .....	110
Não sei como excluir ou cancelar a conta .....	110
Não vejo o botão Encerrar conta na página Contas .....	111
Encerrei minha conta, mas ainda não recebi uma confirmação por e-mail .....	111
Eu recebo um erro ConstraintViolationException "" ao tentar fechar minha conta .....	111
Recebo o erro "CLOSE_ACCOUNT_QUOTA_EXCEEDED" ao tentar encerrar uma conta- membro .....	111
Preciso excluir minha AWS organização antes de fechar a conta de gerenciamento? .....	112
Outros problemas .....	112
Preciso trocar o cartão de crédito do meu Conta da AWS .....	112
Preciso denunciar atividades fraudulentas Conta da AWS .....	112
Eu preciso fechar meu Conta da AWS .....	113
Encerrar a conta .....	114
O que você precisa saber antes de encerrar a conta .....	114
Como encerrar uma conta .....	116
O que esperar depois de encerrar a conta .....	119
Período pós-encerramento .....	120
Reabrindo seu Conta da AWS .....	120
Referência da API .....	121
Ações .....	123
AcceptPrimaryEmailUpdate .....	125
DeleteAlternateContact .....	130

DisableRegion .....	135
EnableRegion .....	139
GetAccountInformation .....	143
GetAlternateContact .....	149
GetContactInformation .....	155
GetGovCloudAccountInformation .....	159
GetPrimaryEmail .....	165
GetRegionOptStatus .....	169
ListRegions .....	173
PutAccountName .....	178
PutAlternateContact .....	183
PutContactInformation .....	189
StartPrimaryEmailUpdate .....	193
Ações relacionadas .....	197
CreateAccount .....	197
CreateGovCloudAccount .....	197
DescribeAccount .....	197
Tipos de dados .....	197
AlternateContact .....	199
ContactInformation .....	201
Region .....	205
ValidationExceptionField .....	206
Parâmetros gerais .....	206
Erros comuns .....	209
Fazer solicitações de consulta HTTP .....	211
Endpoints .....	212
HTTPS obrigatório .....	212
Assinar solicitações da API de gerenciamento de AWS contas .....	212
Cotas .....	213
Gerenciar contas na Índia .....	215
Crie um Conta da AWS com a AWS Índia .....	215
Gerenciar suas informações de verificação do cliente .....	218
Verificar o status da sua verificação do cliente .....	218
Criar suas informações de verificação do cliente .....	218
Editar suas informações de verificação do cliente .....	219
Documentos da Índia aceitos para verificação do cliente .....	220

---

Gerencie sua AWS conta na Índia .....	221
Histórico do documento .....	222
.....	CCXXV

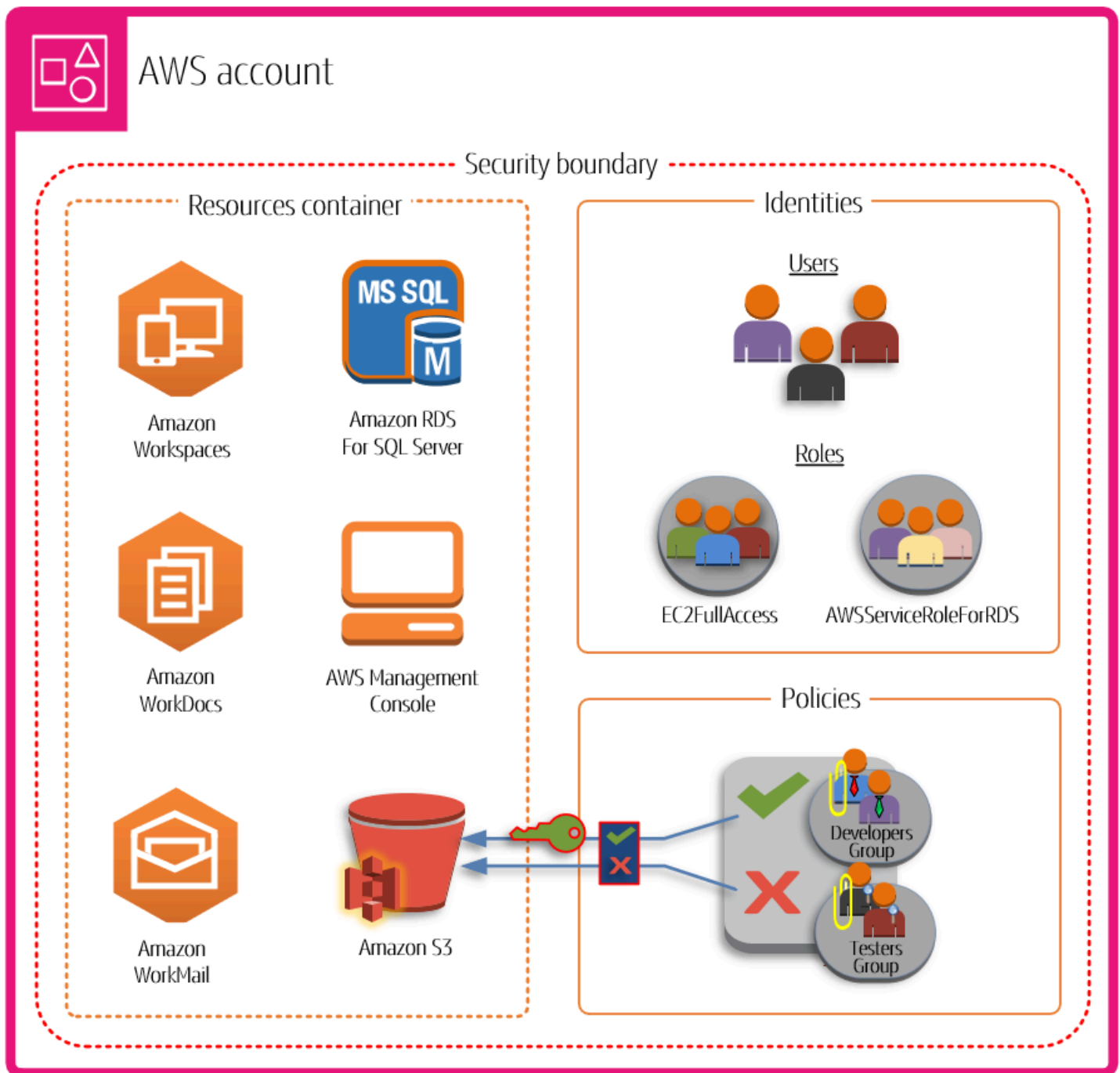
# O que é um Conta da AWS?

An Conta da AWS representa uma relação comercial formal com a qual você estabelece AWS. Você cria e gerencia seus AWS recursos em um Conta da AWS, e sua conta fornece recursos de gerenciamento de identidade para acesso e cobrança. Cada um Conta da AWS tem um ID exclusivo que o diferencia dos outros Contas da AWS.

Seus recursos e dados na nuvem estão contidos em uma Conta da AWS. Uma conta atua como um limite de isolamento do gerenciamento de identidade e acesso. Quando precisar compartilhar recursos e dados entre duas contas, você deverá explicitamente permitir esse acesso. Por padrão, nenhum acesso é permitido entre contas. Por exemplo, se você designar contas diferentes para conter seus recursos e dados de produção e não produção, nenhum acesso será permitido entre esses ambientes, por padrão.

Contas da AWS também são uma parte fundamental do acesso aos AWS serviços. Conforme mostrado na ilustração a seguir, o Conta da AWS an tem duas funções principais:

- **Contêiner de recursos** — 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 EC2 (Amazon) são todos recursos. Cada recurso é identificado exclusivamente por um nome do recurso da Amazon (ARN) que inclui o ID da conta que contém ou possui o recurso.
- **Limite de segurança** — Um também Conta da AWS é o limite básico de segurança para seus AWS recursos. Os recursos que você cria na conta estão disponíveis para os usuários que têm credenciais desta conta. Entre os principais recursos que você pode criar na conta estão as identidades, como usuários e perfis. Essas identidades têm credenciais que alguém pode usar para fazer login (ou autenticar-se) na AWS. As identidades também têm políticas de permissão que especificam o que um usuário pode fazer (autorização) com os recursos da conta.



Usar várias Contas da AWS é uma prática recomendada para escalar seu ambiente, pois fornece um limite natural de faturamento para custos, isola recursos para fins de segurança, oferece flexibilidade para indivíduos e equipes, além de ser adaptável a novos processos de negócios. Para obter mais informações, consulte [Benefícios do uso de várias Contas da AWS](#).

# Características de um Conta da AWS

Contas da AWS incluem os seguintes recursos principais:

- **Monitore e controle os custos** — Uma conta é o meio padrão pelo qual AWS os custos são alocados. Por esse motivo, o uso de contas diferentes para diferentes unidades de negócios e grupos de workloads pode ajudar você a rastrear, controlar, prever, orçar e relatar com mais facilidade suas despesas com a nuvem. Além dos relatórios de custos no nível da conta, AWS também possui suporte integrado para consolidar e relatar custos em todo o conjunto de contas, caso você opte por usá-las AWS Organizations em algum momento. Você também pode usar o AWS Service Quotas para ajudar na proteção contra o provisionamento excessivo inesperado de recursos da AWS e de ações mal-intencionadas que podem afetar drasticamente os custos da AWS.
- **Unidade de isolamento** — Conta da AWS A fornece limites de segurança, acesso e cobrança para seus AWS recursos, o que pode ajudá-lo a obter autonomia e isolamento de recursos. Por padrão, todos os recursos provisionados em uma conta são logicamente isolados dos recursos provisionados em outras contas, mesmo dentro do seu próprio ambiente. AWS Esse limite de isolamento fornece uma maneira de limitar os riscos de um problema relacionado à aplicação, a uma configuração incorreta ou a ações mal-intencionadas. Se ocorrer um problema em uma conta, os impactos nas workloads contidas em outras contas poderão ser reduzidos ou eliminados.
- **Espelhar workloads de negócios**: use várias contas para agrupar workloads com um objetivo comum de negócios em contas distintas. Como resultado, você pode alinhar a propriedade e a tomada de decisões com essas contas e evitar dependências e conflitos com a forma como as workloads de outras contas são protegidas e gerenciadas. Dependendo do seu modelo geral de negócios, você pode optar por isolar unidades de negócios ou subsidiárias distintas em contas diferentes. Essa abordagem também pode facilitar a alienação dessas unidades ao longo do tempo.

## Você é um AWS usuário iniciante?

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

Para step-by-step obter instruções sobre como configurar uma nova conta, consulte [Começando com um Conta da AWS](#).

## AWS Serviços relacionados

Contas da AWS trabalhe perfeitamente com os seguintes serviços:

- IAM

Você Conta da AWS está intimamente integrado ao AWS Identity and Access Management (IAM). Você pode usar o IAM com a conta para garantir que outras pessoas que trabalham na conta tenham o acesso necessário para a conclusão dos seus trabalhos. Você também usa o IAM para controlar o acesso a todos os seus AWS recursos, não apenas às informações específicas da conta. É importante que você se familiarize com os principais conceitos e com as práticas recomendadas do IAM antes de avançar muito na configuração da estrutura da Conta da AWS. Para obter mais informações, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

- AWS Organizations

Se sua empresa é grande ou tem probabilidade de crescer, convém configurar várias AWS contas que reflitam a estrutura específica da sua empresa. AWS Organizations fornece a infraestrutura e os recursos subjacentes para você criar e gerenciar seus ambientes com várias contas. Você pode combinar suas contas existentes em uma organização que permite gerenciar as contas de forma centralizada. Você pode criar contas que automaticamente façam parte de sua organização e convidar outras contas para ingressar nela. Você também pode anexar políticas que afetam algumas ou todas as suas contas. Para obter mais informações, consulte [Quando usar AWS Organizations](#).

- AWS Control Tower

AWS Control Tower fornece uma maneira simplificada de configurar e controlar um ambiente seguro com várias contas AWS . AWS Control Tower automatiza a criação de seu ambiente de várias contas usando AWS Organizations, instanciando um conjunto de contas iniciais e com algumas proteções e configurações padrão para o ambiente. Você pode usar AWS Control Tower para provisionar novas Contas da AWS em algumas etapas e, ao mesmo tempo, garantir que as contas estejam em conformidade com suas políticas organizacionais. Para obter mais informações, consulte [Quando usar AWS Control Tower](#).

# Usando o Usuário raiz da conta da AWS

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em [Tarefas que exigem credenciais de usuário-raiz](#) no Guia do usuário do IAM.

Para evitar o uso do usuário-raiz nas tarefas diárias, saiba como [configurar um usuário administrativo no AWS IAM Identity Center](#). Para obter mais recomendações de segurança do usuário raiz, consulte [As práticas recomendadas do usuário raiz para a Conta da AWS](#).

## Important

Qualquer pessoa que tenha suas credenciais de usuário root Conta da AWS tem acesso irrestrito a todos os recursos da sua conta, incluindo informações de cobrança.

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

## Support for AWS Account Management

Você pode publicar feedback e perguntas usando o [AWS Account Management support forum](#). Para obter informações gerais sobre AWS fóruns, consulte [AWS re:Post](#).

Se não conseguir encontrar as respostas que procura AWS re:Post, você pode criar um caso de suporte relacionado à conta ou cobrança usando o Console de gerenciamento da AWS Para obter mais informações, consulte [Example: Create a support case for account and billing](#).

## Outros AWS recursos

- [AWS Treinamento e cursos](#) — Links para cursos especializados e baseados em funções, bem como laboratórios individualizados para ajudar a aprimorar suas AWS habilidades e ganhar experiência prática.

- [AWS Ferramentas para desenvolvedores](#) — Links para ferramentas e recursos para desenvolvedores que fornecem documentação, exemplos de código, notas de versão e outras informações para ajudá-lo a criar aplicativos inovadores AWS.
- [AWS Support Center](#) — O hub para criar e gerenciar seus casos de AWS Support. Também inclui links para outros recursos úteis, como fóruns, informações técnicas FAQs, status de integridade do serviço e AWS Trusted Advisor.
- [AWS Support](#) — A principal página da web com informações sobre o AWS Support one-on-one, um canal de suporte de resposta rápida para ajudá-lo a criar e executar aplicativos na nuvem.
- [Fale conosco](#) — Um ponto de contato central para consultas sobre AWS faturamento, conta, eventos, abuso e outros problemas.
- [AWS Termos do site](#) — Informações detalhadas sobre nossos direitos autorais e nossa marca registrada; sua conta, licença e acesso ao site; e outros tópicos.

# Começando com um Conta da AWS

Se você é novo em AWS, a primeira etapa é se inscrever em um Conta da AWS. Quando você fizer isso, a AWS criará uma conta usando os detalhes que você forneceu e a atribuirá a você.

Os tópicos desta seção ajudarão você a começar a aprender e a configurar um novo Conta da AWS.

## Tópicos

- [Pré-requisitos para criar um novo Conta da AWS](#)
- [Crie um Conta da AWS](#)
- [Ativar a MFA para o usuário-raiz](#)
- [Criação de um usuário administrador](#)
- [Acessando seu Conta da AWS](#)

## Pré-requisitos para criar um novo Conta da AWS

Para se inscrever em um Conta da AWS, você precisará fornecer as seguintes informações:

- **Endereço de e-mail do usuário-raiz:** esse endereço de e-mail é usado como nome de login do [usuário-raiz](#) e é necessário para a recuperação da conta. Você precisa poder receber mensagens de e-mail que sejam enviadas para esse endereço. Antes de poder executar determinadas tarefas, você precisa verificar se tem acesso a e-mails enviados para esse endereço.
- **AWS nome da 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 dar nome às contas para poder 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).
- **Endereço** — Se seu endereço de contato e cobrança for na Índia, o contrato de usuário da sua conta é com a Amazon Web Services India Private Limited (AWS Índia), um vendedor AWS 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. AWS A Índia cobra 2 INR de sua forma de pagamento como parte do processo de verificação. AWS A Índia reembolsa os 2 INR após a conclusão da verificação.

- Número de telefone: esse número é usado para fins de verificação de identidade e para confirmar a propriedade da conta. Ele precisa estar disponível para receber chamadas e mensagens de SMS.

#### 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.

## Crie um Conta da AWS

Essas instruções são para criar um ambiente Conta da AWS fora da Índia. Para criar uma conta na Índia, consulte [Crie um Conta da AWS com a AWS Índia](#). Para criar uma conta que faz parte de uma organização gerenciada por AWS Organizations, consulte [Criação de uma conta de membro em uma organização](#) no Guia AWS Organizations do usuário.

### Console de gerenciamento da AWS

Para criar um Conta da AWS


1. Abra a página [Cadastrar-se na AWS](#).
2. Insira o endereço de e-mail e o Conta da AWS nome do usuário raiz e escolha Verificar endereço de e-mail. Com isso, será enviado um código de verificação para seu endereço de e-mail especificado.

#### 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.

3. Insira seu código de verificação e escolha Verificar.

4. Insira uma senha forte para seu usuário root, confirme-a e escolha Continuar. AWS exige 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 deve ser idêntico ao seu Conta da AWS nome ou endereço de e-mail.
5. Escolha Comercial ou Pessoal. Contas pessoais e comerciais têm os mesmos recursos e funções.
6. Insira suas informações pessoais ou da empresa.

 Important

Para empresas Contas da AWS, é uma prática recomendada inserir o número de telefone da empresa em vez do número de um telefone pessoal. Configurar o usuário-raiz da conta com um endereço de e-mail individual ou um número de telefone pessoal pode tornar a conta insegura.

7. Leia e aceite o [Contrato do cliente da AWS](#). Certifique-se de ler e entender os termos do Contrato do AWS Cliente.
8. Escolha Continuar. Nesse momento, você receberá uma mensagem de e-mail confirmando que Conta da AWS está pronto para uso. Você pode fazer login na sua nova conta usando o endereço de e-mail e a senha que forneceu durante o cadastro. No entanto, você não pode usar nenhum AWS serviço até terminar de ativar sua conta.
9. Insira as informações sobre seu método 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 poderá continuar com o processo de cadastro até adicionar um método de pagamento válido.

10. Insira o código do seu país ou região na lista e insira um número de telefone no qual você possa receber ligações nos próximos minutos.
11. Insira o código exibido no CAPTCHA e, em seguida, envie.
12. Quando o sistema automatizado entrar em contato com você, insira o PIN que você recebeu e envie.

13. Selecione um dos AWS Support planos disponíveis. Para obter uma descrição dos planos de suporte disponíveis e seus benefícios, consulte [Comparar planos Suporte](#).
14. Escolha Concluir cadastramento. É exibida uma página de confirmação indicando que sua conta está sendo ativada.
15. Verifique suas pastas de e-mail e de spam para encontrar uma mensagem de e-mail que confirme sua conta foi ativada. A ativação geralmente leva alguns minutos mas, às vezes, pode demorar até 24 horas.
16. Depois de receber a mensagem de ativação, você pode entrar no para começar a [Console de gerenciamento da AWS](#)usar. Serviços da AWS Para obter informações gerais sobre como gerenciar suas configurações de conta, consulte [Configure seu Conta da AWS](#).

## AWS CLI & SDKs

Você pode criar contas de membros em uma organização gerenciada AWS Organizations executando a [CreateAccount](#) operação 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.

## Ativar a MFA para o usuário-raiz

É altamente recomendável que você ative a MFA no usuário-raiz. A MFA reduz drasticamente o risco de alguém acessar sua conta sem sua autorização.

1. Faça login [Console de gerenciamento da AWS](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda para fazer login usando seu usuário root, consulte [Fazer login Console de gerenciamento da AWS como usuário root no](#) Guia do usuário AWS de login.

2. Ativar MFA para o usuário-raiz.

Para obter instruções, consulte [Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz \(console\) no Guia](#) do usuário do IAM.

## Criação de um usuário administrador

Como não é possível restringir o que um usuário-raiz pode fazer, é altamente recomendável que você não use o usuário-raiz para tarefas que não exijam explicitamente o usuário-raiz. Em vez disso, atribua acesso administrativo a um usuário administrativo no Centro de Identidade do IAM e faça login como usuário administrativo para executar as 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 as credenciais de usuário-raiz, consulte [Proteger as credenciais do usuário-raiz](#) no Guia do usuário do IAM.
- Para obter uma lista de tarefas que exigem usuário-raiz, consulte [Tarefas que exigem credenciais do usuário-raiz](#) no Guia do Usuário do IAM.

## Acessando seu Conta da AWS

Você pode acessar o seu Conta da AWS de qualquer uma das seguintes formas:

### Console de gerenciamento da AWS

[Console de gerenciamento da AWS](#) É uma interface baseada em navegador que você pode usar para gerenciar suas Conta da AWS configurações e seus AWS recursos.

### AWS Ferramentas de linha de comando

Com as ferramentas de linha de AWS comando, você pode emitir comandos na linha de comando do seu sistema para executar Conta da AWS AWS tarefas. Usar a linha de comando pode ser mais rápido e mais conveniente do que o console. As ferramentas de linha de comando também são úteis se você quiser criar scripts que executem AWS tarefas. AWS fornece dois conjuntos de ferramentas de linha de comando:

- [AWS Command Line Interface](#)(AWS CLI). Para obter informações sobre como instalar e usar o AWS CLI, consulte o [Guia AWS Command Line Interface do usuário](#).
- [AWS Tools for Windows PowerShell](#). Para obter informações sobre como instalar e usar as Ferramentas para Windows PowerShell, consulte o [Guia Ferramentas da AWS para PowerShell do Usuário](#).

## AWS SDKs

Eles AWS SDKs consistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação (por exemplo, Java, Python, Ruby, .NET, iOS e Android). Eles SDKs cuidam de tarefas como assinar criptograficamente solicitações, gerenciar erros e repetir solicitações automaticamente. Para obter mais informações sobre o AWS SDKs, incluindo como baixá-los e instalá-los, consulte [Ferramentas para Amazon Web Services](#).

### AWS API de consulta HTTPS de gerenciamento de contas

A API de consulta HTTPS de gerenciamento de AWS contas fornece acesso programático ao seu Conta da AWS e. AWS A API de consulta HTTPS permite que você execute solicitações HTTPS diretamente para o serviço. Quando você usa a API HTTPS, deve incluir código para assinar digitalmente solicitações usando suas credenciais. Para obter mais informações, consulte [Calling the API by making HTTP Query requests](#).

# Planeje sua estrutura de Conta da AWS governança

Embora você possa ter iniciado sua AWS jornada com uma única conta, AWS recomenda que você configure várias contas à medida que suas cargas de trabalho aumentam em tamanho e complexidade. Se você é uma empresa de médio ou de grande porte, convém criar um plano de estrutura de governança que garanta que as necessidades de dados e de workload sejam atendidas.

Esta seção aborda os benefícios e os serviços de governança disponíveis AWS para ajudar a viabilizar uma estrutura de governança de várias contas.

## Tópicos

- [Benefícios do uso de vários Contas da AWS](#)
- [Quando usar AWS Organizations](#)
- [Quando usar AWS Control Tower](#)
- [Noções básicas dos modos de operação da API](#)

## Benefícios do uso de vários Contas da AWS

Contas da AWS formam o limite de segurança fundamental no. Nuvem AWS Elas atuam como um contêiner para recursos, fornecendo uma camada crítica de isolamento que é essencial para a criação de um ambiente seguro e bem governado. Para obter mais informações, consulte [O que é um Conta da AWS?](#).

Separar seus recursos em partes Contas da AWS ajuda você a apoiar os seguintes princípios em seu ambiente de nuvem:

- Controle de segurança: aplicações diferentes podem ter perfis de segurança diferentes, exigindo políticas e mecanismos de controle diferentes. Por exemplo, é muito mais fácil falar com um auditor e ser capaz de apontar para um único Conta da AWS que hospeda todos os elementos de sua carga de trabalho que estão sujeitos aos padrões de segurança do [setor de cartões de pagamento \(PCI\)](#).
- Isolamento — An Conta da AWS é uma unidade de proteção de segurança. Os riscos potenciais e as ameaças à segurança devem estar contidos dentro e Conta da AWS sem afetar os outros. Pode haver necessidades de segurança diferentes devido a equipes ou perfis de segurança diferentes.

- Muitas equipes — equipes diferentes têm responsabilidades e necessidades de recursos diferentes. Você pode evitar que as equipes interfiram umas nas outras movendo-as para uma posição separada Contas 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 na conformidade com o [Regulamento Geral de Proteção de Dados \(GDPR\) da União Europeia](#).
- Processo de negócios — Diferentes unidades de negócios ou produtos podem ter finalidades e processos completamente diferentes. Com várias Contas da AWS, você pode atender às 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 cobrança entre unidades de negócios, equipes funcionais ou usuários individuais. Você ainda pode consolidar todas as suas contas em um único pagador (usando AWS Organizations e consolidando o faturamento) enquanto separa os itens de linha por. Conta da AWS
- Alocação de cotas — as cotas AWS de serviço são aplicadas separadamente para cada uma. Conta da AWS Separar as workloads em diferentes Contas da AWS impede que elas consumam cotas umas das outras.

Todas as recomendações e procedimentos descritos neste documento estão em conformidade com o [Framework Well-Architected da AWS](#). Essa estrutura tem como objetivo ajudar você a projetar uma infraestrutura de nuvem flexível, resiliente e escalável. Mesmo quando você está começando aos poucos, recomendamos que prossiga de acordo com estas orientações da estrutura. Isso pode ajudar a escalar seu ambiente com segurança e sem afetar suas operações contínuas à medida que a empresa cresce.

## Gerenciando vários Contas da AWS

Antes de começar a adicionar várias contas, você deve desenvolver um plano para gerenciá-las. Para isso, recomendamos que você use [AWS Organizations](#), que é um AWS serviço gratuito para gerenciar tudo Contas da AWS em sua organização.

AWS também oferece AWS Control Tower, que adiciona camadas de automação AWS gerenciada ao Organizations e a integra automaticamente a outros AWS serviços AWS CloudTrail AWS Config,

como Amazon CloudWatch e outros. AWS Service Catalog Esses serviços podem incorrer em custos adicionais. Para obter mais informações, consulte [Preços do AWS Control Tower](#).

## Consulte também

- [Quando usar AWS Organizations](#)
- [Quando usar AWS Control Tower](#)

## Quando usar AWS Organizations

AWS Organizations é um AWS serviço que você pode usar para gerenciar seu Contas da AWS grupo. Isso fornece recursos, como faturamento consolidado, em que todas as faturas das contas são agrupadas e administradas por um pagante. Você também pode gerenciar de forma centralizada a segurança da organização usando controles baseados em políticas. Para obter mais informações sobre AWS Organizations, consulte o [Guia AWS Organizations do usuário](#).

### 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 só inclui as operações relacionadas ao gerenciamento da própria organização. Você pode estender essa funcionalidade adicional a outros AWS serviços ao permitir o acesso confiável entre Organizations 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 ao Organizations e à conta de gerenciamento dele permissões para acessar os metadados, como as informações de contato primário ou alternativo, de todas as contas-membro da organização.

Para obter mais informações, consulte [Habilite o acesso confiável para o gerenciamento de AWS contas](#).

### Administrador delegado

Depois de habilitar o acesso confiável, você também pode escolher designar uma de suas contas de membro como uma conta de administrador delegada 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-membro na organização que,

anteriormente, somente a conta de gerenciamento podia fazer. A conta de administrador delegado só pode acessar 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 gerenciamento de AWS contas](#).

### Políticas de controle de serviço

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

Por exemplo, SCPs que se aplicam a Contas da AWS, consulte [Restrinja o acesso usando políticas AWS Organizations de controle de serviços](#).

## Habilite o acesso confiável para o gerenciamento de AWS contas

Habilitar o acesso confiável para o Gerenciamento de AWS 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 em AWS Organizations. Para obter mais informações, consulte [AWS Account Management and AWS Organizations](#) no AWS Organizations User Guide. Para obter informações gerais sobre como o acesso confiável funciona, consulte [Usando AWS Organizations com outros AWS serviços](#).

Depois que o acesso confiável tiver sido habilitado, você poderá usar o parâmetro `accountID` nas [operações da API de Gerenciamento de Contas](#) compatíveis. Você só poderá usar esse parâmetro com êxito 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 gerenciamento de AWS contas](#).

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

### Permissões mínimas

Para executar essas tarefas, você deve atender aos seguintes requisitos:

- Você só pode executar essas tarefas na conta de gerenciamento da organização.
- A organização deve ter [todos os recursos habilitados](#).

## Console de gerenciamento da AWS

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. No painel de navegação, escolha Serviços.
3. Escolha Gerenciamento de Contas da AWS 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 habilitar 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 parâmetro `--accountId` para fazer referência às contas-membro de uma organização.

- AWS CLI: [enable-aws-service-access](#)

O exemplo a seguir permite 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 gerenciamento de AWS contas

Você ativa uma conta de administrador delegado para poder chamar as operações da API de gerenciamento de AWS contas para outras contas de membros em AWS Organizations. Depois de registrar uma conta de administrador delegado para sua organização, os usuários e funções dessa conta podem chamar as operações do SDK AWS CLI e do AWS SDK no account namespace que podem funcionar no modo Organizations oferecendo suporte a um parâmetro opcional. AccountId

Para registrar uma conta-membro na organização como conta de administrador delegado, use o procedimento a seguir.

### AWS CLI & SDKs

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

Use os comandos a seguir para habilitar um administrador delegado para o serviço de Gerenciamento de Contas.

#### Permissões mínimas

Para executar essas tarefas, você deve atender aos seguintes requisitos:

- Você só pode executar essas tarefas na conta de gerenciamento da organização.
- A organização deve ter [todos os recursos habilitados](#).
- É preciso que tenha sido [habilitado acesso confiável para o Gerenciamento de Contas na organização](#).

Você deve especificar a seguinte entidade principal de serviço:

```
account.amazonaws.com
```

- AWS CLI: [register-delegated-administrator](#)

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

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

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

Depois de executar esse comando, você pode usar as credenciais da conta 123456789012 para chamar as operações de gerenciamento de contas AWS CLI e da API do SDK que usam o `--account-id` parâmetro para referenciar contas de membros em uma organização.

## Console de gerenciamento da AWS

Essa tarefa não é suportada no console de gerenciamento de AWS contas. Você pode realizar essa tarefa somente usando o AWS CLI ou uma operação de API de um dos AWS SDKs.

## Restrinja o acesso usando políticas AWS Organizations de controle de serviços

Este tópico apresenta exemplos que mostram como você pode usar políticas de controle de serviço (SCPs) AWS Organizations para restringir o que os usuários e funções nas contas da sua organização podem fazer. Para obter mais informações sobre políticas de controle de serviços, consulte os seguintes tópicos no AWS Organizations User Guide:

- [Criando SCPs](#)
- [Anexação SCPs OUs e contas](#)
- [Estratégias para SCPs](#)
- [Sintaxe da política de SCP](#)

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

O exemplo a seguir impede que as operações de API `PutAlternateContact` e `DeleteAlternateContact` sejam chamadas por qualquer conta-membro no [modo de conta](#)

[autônoma](#). Isso impede que qualquer entidade principal das contas afetadas altere seus próprios contatos alternativos.

## JSON

```
{
  "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-membro modifique contatos alternativos para qualquer outra conta-membro da organização

O exemplo a seguir generaliza o elemento Resource como "\*", o que significa que ele se aplica tanto às [solicitações do modo autônomo quanto às solicitações do modo organizações](#). Isso significa que até mesmo a conta de administrador delegado para o Gerenciamento de Contas, se a SCP se aplicar a ela, estará impedida de alterar qualquer contato alternativo para qualquer conta da organização.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
```

```
        "account:DeleteAlternateContact"  
      ],  
      "Resource": [ "*" ]  
    }  
  ]  
}
```

Example Exemplo 3: impedir que uma conta-membro de uma UO 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 especificada OUs de modificar seus próprios contatos alternativos.

## Quando usar AWS Control Tower

AWS Organizations é o serviço básico que permite gerenciar e proteger de forma centralizada todo o AWS seu ambiente. Um componente crucial dessa abordagem AWS Organizations centrada é. AWS Control Tower AWS Control Tower atua como um console de gerenciamento dentro do Organizations, fornecendo uma maneira simplificada de configurar e governar um AWS ambiente seguro com várias contas aplicando as melhores práticas prescritivas.

Essa abordagem de melhores práticas de segurança fornecida pela AWS Control Tower amplia os principais recursos do AWS Organizations. AWS Control Tower aplica um conjunto de proteções preventivas e de detecção para ajudar a garantir que sua organização e suas contas permaneçam alinhadas com os padrões recomendados de segurança e conformidade.

Ao estabelecer uma AWS Organizations estrutura bem arquitetada com AWS Control Tower, você pode implantar rapidamente um ambiente escalável, seguro e compatível. AWS Essa abordagem centralizada de gerenciamento e governança da nuvem é essencial para empresas que desejam aproveitar todo o poder da e, Nuvem AWS ao mesmo tempo, manter os mais altos padrões de segurança e conformidade.

Para obter mais informações, consulte [O que é o AWS Control Tower?](#) no Manual do usuário do AWS Control Tower .

## Noções básicas dos modos de operação da API

As operações de API que funcionam com os atributos Conta da AWS de an sempre funcionam em um dos dois modos de operação:

- **Contexto autônomo:** esse modo é usado quando um usuário ou perfil de uma conta acessa ou altera um atributo da mesma conta. O modo de contexto autônomo é usado automaticamente quando você não inclui o `AccountId` parâmetro ao chamar uma das operações de gerenciamento de contas AWS CLI ou AWS SDK.
- **Contexto de organizações:** esse modo é usado quando um usuário ou perfil de uma conta de uma organização acessa ou altera um atributo de uma conta-membro diferente da mesma organização. O modo de contexto da organização é usado automaticamente quando você inclui o `AccountId` parâmetro ao chamar uma das operações de gerenciamento de contas AWS CLI ou AWS SDK. Você só pode chamar as operações nesse modo na conta de gerenciamento da organização ou na conta do administrador delegado para o Gerenciamento de Contas.

As operações do AWS SDK AWS CLI e do SDK podem funcionar em um contexto autônomo ou organizacional.

- Se você não incluir o parâmetro `AccountId`, a operação será executada no contexto autônomo e aplicará automaticamente a solicitação à conta que você usou para fazer a solicitação. Isso é válido independentemente de a conta ser ou não membro de uma organização.
- Se você incluir o parâmetro `AccountId`, a operação será executada no contexto de organizações e funcionará na conta especificada do Organizations.
  - Se a conta que estiver chamando a operação for a conta de gerenciamento ou a conta do administrador delegado para o serviço de Gerenciamento de Contas, você poderá especificar qualquer conta-membro dessa organização no parâmetro `AccountId` para atualizar a conta especificada.
  - A única conta de uma organização que pode chamar uma das operações de contato alternativo e especificar seu próprio número de conta no parâmetro `AccountId` é a conta especificada como a [conta do administrador delegado](#) para o serviço de Gerenciamento de Contas. Qualquer outra conta, incluindo a conta de gerenciamento, recebe uma exceção `AccessDenied`.
- Se você executar uma operação no modo autônomo, deverá ter permissão para executar a operação com uma política do IAM que inclua um elemento `Resource` de qualquer "\*" para permitir todos os recursos ou um [ARN que use a sintaxe para uma conta independente](#).

- Se você executar uma operação no modo de organizações, deverá ter permissão para executar a operação com uma política do IAM que inclua um elemento Resource de qualquer "\*" para permitir todos os recursos ou um [ARN que use a sintaxe para uma conta-membro de uma organização](#).

## Conceder permissões para atualizar atributos da conta

Como na maioria das AWS operações, você concede permissões para adicionar, atualizar ou excluir atributos da conta Contas da AWS usando [políticas de permissão do IAM](#). Ao anexar uma política de permissão do IAM a uma entidade principal do IAM (um usuário ou um perfil), você especifica quais ações essa entidade principal pode executar em quais recursos e sob quais condições.

A seguir são mostradas algumas considerações específicas do Gerenciamento de Contas para a criação de uma política de permissões.

### Formato de nome de recurso da Amazon para Contas da AWS

- O [Amazon Resource Name \(ARN\)](#) de um Conta da AWS que você pode incluir no 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 independente ou uma conta que está em uma organização. Consulte a seção anterior em [Noções básicas dos modos de operação da API](#).

- Um ARN de conta para uma conta autônoma:

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

Você deve usar esse formato quando executar uma operação de atributos de conta no modo autônomo, não incluindo o parâmetro Account ID.

- Um ARN de conta para uma conta-membro em uma organização:

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

Você deve usar esse formato quando executar uma operação de atributos de conta em organizações, incluindo o parâmetro Account ID.

## Chaves de contexto para políticas do IAM

O serviço de Gerenciamento de Contas também fornece várias [chaves de condição específicas do serviço de Gerenciamento de Contas](#) que fornecem controle refinado sobre as permissões que você concede.

### **account:AccountResourceOrgPaths**

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

Como `account:AccountResourceOrgPaths` é um tipo de string multivalor, você deve usar os operadores de string de vários valores [ForAnyValue ou ForAllValues](#). Além disso, observe que o prefixo na chave de condição é `account`, mesmo que você esteja referenciando caminhos para uma OUs 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 key/value de sequências que você pode usar para categorizar e rotular os recursos em sua conta. Para obter mais informações sobre marcação, consulte [Tag Editor](#) no AWS Resource Groups User Guide. Para obter informações sobre o uso de tags como parte de uma estratégia de controle de acesso baseado em atributos, consulte [What is ABAC for AWS](#) no Guia do usuário do IAM. O exemplo de trecho seguir restringe a política para ser aplicada somente a contas de uma organização que tenham a tag com a chave `project` e um valor de `blue` ou `red`.

Como `account:AccountResourceOrgTags` é um tipo de string multivalor, você deve usar os operadores de string de vários valores [ForAnyValue](#) ou [ForAllValues](#). Além disso, observe que o prefixo da chave de condição é `account`, mesmo que você esteja fazendo referência às tags de uma conta-membro da organização.

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

#### Note

Você pode anexar tags a apenas uma conta de uma organização. Você não pode anexar etiquetas a um arquivo autônomo. Conta da AWS

# Configure seu Conta da AWS

Esta seção inclui tópicos que descrevem como gerenciar seu Conta da AWS.

## Note

Se você Conta da AWS foi criado na Índia usando a Amazon Web Services India Private Limited (AWS Índia), há outras considerações. Para obter mais informações, consulte [Gerenciar contas na Índia](#).

## Tópicos

- [Crie um Conta da AWS alias](#)
- [Ativar ou desativar Regiões da AWS em sua conta](#)
- [Atualize o faturamento do seu Conta da AWS](#)
- [Atualize o endereço de e-mail do usuário-raiz](#)
- [Atualizar senha do usuário-raiz](#)
- [Atualize seu Conta da AWS nome](#)
- [Atualize os contatos alternativos para o seu Conta da AWS](#)
- [Atualize o contato principal do seu Conta da AWS](#)
- [Exibir Conta da AWS identificadores](#)

## Crie um 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 [usar um alias para sua Conta da AWS ID no Guia](#) do usuário do IAM.

## Ativar ou desativar Regiões da AWS em sua conta

An Região da AWS é um local físico no mundo com AWS 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. Executar cargas de trabalho em um local Região da AWS mais próximo dos usuários finais pode melhorar o desempenho e diminuir a latência. Para obter um mapa das regiões disponíveis e futuras, consulte [Regiões e zonas de disponibilidade](#). Para saber mais sobre a arquitetura Regiões da AWS de resiliência para suas cargas de trabalho, visite Fundamentos de [AWS várias](#) regiões.

Regiões da AWS geralmente se enquadram em duas categorias de disponibilidade para contas:

- Regiões padrão: regiões lançadas antes de 20 de março de 2019 são habilitadas por padrão. Você pode criar e gerenciar recursos nessas regiões padrão imediatamente após a ativação da sua conta. As regiões padrão não podem ser habilitadas ou desabilitadas.
- Regiões de aceitação: regiões lançadas após 20 de março de 2019 são desabilitadas por padrão e são chamadas regiões de aceitação. As regiões de aceitação desativadas não são mostradas na barra de navegação do console e você não pode usar essas regiões para criar workloads até que estejam habilitadas. Para usar essas regiões opcionais, você deve primeiro habilitá-las em seu Conta da AWS. Depois de habilitar uma região de aceitação, será possível selecionar essa região na barra de navegação e criar e gerenciar recursos nessa região. Para habilitar a região de aceitação para suas contas autônomas, consulte [Habilitar ou desabilitar região para contas autônomas](#) e para habilitar a região de aceitação para suas contas de membros, consulte [Habilitar ou desabilitar uma região na organização](#).

Quando você se inscreve em uma Conta da AWS, AWS recomenda uma região de inscrição para você com base no país do seu endereço de contato. Clientes em um país com uma região de AWS aceitação veem uma recomendação na página de informações de contato para ativar a região de aceitação nesse país. Clientes em um país com uma região de aceitação e uma região padrão, como Índia, Austrália ou Canadá, recebem uma recomendação para selecionar a região de aceitação se a região de aceitação estiver mais próxima deles do que a região padrão. Depois que uma conta é ativada, você pode ativar outras regiões de AWS aceitação em sua conta ou optar por desativar a região de inscrição que você ativou durante a inscrição.

Quando você cria um Conta da AWS, seus dados e credenciais do IAM são configurados automaticamente para funcionar em todas as regiões padrão, permitindo que o usuário raiz e as identidades do IAM com as permissões apropriadas acessem AWS os serviços nessas regiões usando suas credenciais existentes. AWS As regiões opt-in são desativadas por padrão, e os dados e credenciais do IAM não estão disponíveis inicialmente nessas regiões, o que impede o acesso

aos AWS serviços nessa região. Quando você escolhe habilitar uma região de aceitação, a AWS propaga seus dados e credenciais do IAM para essa região. Depois que a propagação for concluída e a região de aceitação estiver ativada, o usuário raiz e as identidades do IAM poderão acessar os AWS serviços na região de aceitação recém-ativada usando as mesmas credenciais do IAM que usam nas regiões padrão.

Quando você desabilita uma região de aceitação, suas credenciais do IAM são desabilitadas e você perde o acesso do IAM aos recursos dessa região. A desabilitação de uma região de aceitação não exclui os recursos dessa região e as cobranças por recursos (se houver) nessa região de aceitação desabilitada continuam sendo acumuladas na taxa padrão.

#### Important

A desativação de uma região desativa o acesso do IAM aos recursos na região. Isso não exclui os recursos em questão, que continuam incorrendo em cobranças. Remova todos os recursos restantes antes de desativar uma região.

AWS agrupa regiões em [partições](#). Cada região está em exatamente uma partição, e cada partição tem uma ou mais regiões. As partições têm instâncias independentes de AWS Identity and Access Management (IAM) e fornecem um limite rígido entre regiões em partições diferentes. AWS As regiões comerciais estão na `aws` partição, as regiões na China estão na `aws-cn` partição e AWS GovCloud (US) as regiões estão na `aws-us-gov` partição. Dependendo da partição em que você criou sua Conta da AWS, você pode usá-la Regiões da AWS dentro dessa partição.

- Uma conta na `aws` partição fornece acesso a várias regiões na partição comercial para que você possa lançar AWS recursos em locais que atendam às suas necessidades. Por exemplo, talvez você queira executar instâncias do Amazon EC2 na Europa para estar mais próximo dos seus clientes europeus ou para cumprir requisitos jurídicos.
- Uma conta na `aws-us-gov` partição fornece acesso à região AWS GovCloud (Oeste dos EUA) e à região AWS GovCloud (Leste dos EUA). Para obter mais informações, consulte [AWS GovCloud \(US\)](#).
- Uma conta na partição `aws-cn` fornece acesso somente às regiões Pequim e Ningxia. Para obter mais informações, consulte [Amazon Web Services na China](#).

## Tópicos

- [Referência de disponibilidade regional](#)

- [Considerações antes de habilitar e desabilitar regiões](#)
- [Tempos de processamento e limites de solicitação](#)
- [Habilitar ou desabilitar região para contas autônomas](#)
- [Habilitar ou desabilitar uma região na organização](#)

## Referência de disponibilidade regional

As tabelas a seguir listam Regiões da AWS por tipo de disponibilidade. As regiões padrão são habilitadas automaticamente e não podem ser desabilitadas, enquanto as regiões de aceitação devem ser habilitadas manualmente antes que você possa usá-las:

### Opt-in Regions

As seguintes regiões são regiões de aceitação que devem ser habilitadas antes que você possa usá-las:

Nome	Código	Status
África (Cidade do Cabo)	af-south-1	GA
Ásia-Pacífico (Hong Kong)	ap-east-1	GA
Ásia-Pacífico (Taipei)	ap-east-2	GA
Ásia-Pacífico (Hyderabad)	ap-south-2	GA
Ásia-Pacífico (Jacarta)	ap-southeast-3	GA
Ásia-Pacífico (Melbourne)	ap-southeast-4	GA
Ásia-Pacífico (Malásia)	ap-southeast-5	GA
Ásia-Pacífico (Nova Zelândia)	ap-southeast-6	GA
Ásia-Pacífico (Tailândia)	ap-southeast-7	GA
Oeste do Canadá (Calgary)	ca-west-1	GA
Europa (Zurique)	eu-central-2	GA

Nome	Código	Status
Europa (Milão)	eu-south-1	GA
Europa (Espanha)	eu-south-2	GA
Israel (Tel Aviv)	il-central-1	GA
Oriente Médio (Emirados Árabes Unidos)	me-central-1	GA
Oriente Médio (Bahrein)	me-south-1	GA
México (Centro)	mx-central-1	GA

## Default Regions

As seguintes regiões estão habilitadas por padrão e não podem ser desabilitadas:

Nome	Código
Ásia-Pacífico (Tóquio)	ap-northeast-1
Ásia-Pacífico (Seul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Ásia-Pacífico (Mumbai)	ap-south-1
Ásia-Pacífico (Singapura)	ap-southeast-1
Ásia-Pacífico (Sydney)	ap-southeast-2
Canadá (Central)	ca-central-1
Europa (Frankfurt)	eu-central-1
Europa (Estocolmo)	eu-north-1
Europa (Irlanda)	eu-west-1

Nome	Código
Europa (Londres)	eu-west-2
Europa (Paris)	eu-west-3
América do Sul (São Paulo)	sa-east-1
Leste dos EUA (Norte da Virgínia)	us-east-1
Leste dos EUA (Ohio)	us-east-2
Oeste dos EUA (N. da Califórnia)	us-west-1
Oeste dos EUA (Oregon)	us-west-2

Para obter uma lista de nomes de região e seus respectivos códigos, consulte [Regional endpoints](#) no AWS General Reference Guide. 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 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](#).

## Considerações antes de habilitar e desabilitar regiões

Antes de habilitar ou desabilitar uma região, é importante considerar o seguinte:

- Você pode usar todas as regiões de destino em uma geografia de inferência entre regiões, independentemente do status de opção por região — Alguns serviços AWS generativos de IA, incluindo o Amazon Bedrock ([consulte Aumentar a produtividade com inferência entre regiões](#)) e o Amazon Q Developer ([consulte Processamento entre regiões](#) no Amazon Q Developer) usam inferência [entre regiões](#). Se você usa esses serviços, eles selecionam automaticamente a Região da AWS ideal, incluindo as regiões que você não habilitou para recursos e dados do IAM, dentro da geografia escolhida. Isso melhora a experiência do cliente ao maximizar a disponibilidade da computação e do modelo disponível.
- 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 habilitar e desabilitar 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 e desabilitar uma região é grátis: a habilitação e desabilitação de uma região não é cobrada. Você só receberá uma cobrança pelos recursos que criar na nova região.
- EventBridge Integração com a Amazon — Você pode se inscrever para receber notificações de atualização de status por região em. EventBridge Uma EventBridge notificação será criada para cada alteração de status, permitindo que os clientes automatizem os fluxos de trabalho.
- Status expressivo de aceitação por região — devido à natureza assíncrona de uma região de aceitação, há quatro possíveis status para enabling/disabling uma solicitação de aceitação por região:
  - ENABLING
  - DISABLING
  - ENABLED
  - DISABLED

Você não pode cancelar uma operação de ativação ou desativação que esteja no status ENABLING ou DISABLING. Caso contrário, uma `ConflictException` será lançada. 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.

## Tempos de processamento e limites de solicitação

Ao habilitar ou desabilitar regiões, esteja ciente das seguintes limitações de tempo e solicitação:

- A operação de habilitar uma região leva de alguns minutos a várias horas, em alguns casos: quando você habilita uma região, a AWS executa ações para preparar a conta nesta região, como a distribuição dos recursos do IAM para a região. Esse processo leva alguns minutos para a maioria das contas, mas pode, às vezes, levar várias horas. Você não pode usar a região até que esse processo seja concluído.
- Desabilitar uma região nem sempre é algo imediatamente visível: os serviços e os consoles podem ficar temporariamente visíveis depois que uma região é desabilitada. A operação de desabilitar uma região pode levar de alguns minutos a várias horas para surtir efeito.
- Uma única conta pode ter seis solicitações de opção de ativação ou desativação de regiões em andamento a qualquer momento: uma solicitação equivale a habilitar ou desabilitar uma região específica para uma conta.
- 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 habilitar ou desabilitar uma região específica para uma conta.

## Habilitar ou desabilitar região para contas autônomas

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

### Console de gerenciamento da AWS

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

#### Permissões mínimas

Para executar as etapas do procedimento a seguir, um usuário ou perfil 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 [Console de gerenciamento da AWS](#) como usuário Usuário raiz da conta da AWS ou função do IAM que tenha as permissões mínimas.
2. Escolha o nome da conta no canto superior direito da janela e depois escolha Conta.
3. Na página [Conta](#), role para baixo até a seção Regiões da AWS.
4. Escolha a região que você deseja habilitar e desabilitar e escolha a ação desejada Habilitar ou Desabilitar. Você verá um prompt para confirmar.
5. Se você tiver escolhido a opção Habilitar, analise o texto exibido e escolha Habilitar região.

Se você tiver escolhido a opção Desabilitar, analise o texto exibido, digite **disable** para confirmar e escolha Desabilitar região.

Depois que a região de aceitação for habilitada, você poderá selecionar essa região na barra de navegação da região. Para as etapas de seleção de uma região, consulte [Escolher uma região pela barra de navegação no Console de gerenciamento da AWS](#) e para a configuração específica do console da região em sua conta, consulte [Definir a região padrão no Console de gerenciamento da AWS](#).

## 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, é necessário ter a permissão que é mapeada 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 de ativação e desativação da região e conceder a outros a capacidade de ler e gravar.

O exemplo a seguir habilita uma região para a conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

Você também pode desabilitar uma região usando o mesmo comando e, depois, substituindo `enable-region` 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"
}
```

## Habilitar ou desabilitar uma região na 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 o Gerenciamento de AWS contas para APIs que você possa acessar os dados da conta a partir do AWS Organizations console. Para ver as políticas gerenciadas atualizadas, consulte [Atualizações das políticas AWS gerenciadas da Organizations](#).

### Note

Antes de executar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização para uso com contas-membro, você deve:

- Habilitar todos os recursos na sua organização para gerenciar as configurações das contas-membro. Isso permite o controle administrativo das contas-membro. 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 [Enabling all features in your organization](#).
- Ative o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulte [Habilite o acesso confiável para o gerenciamento de AWS contas](#).

## Console de gerenciamento da AWS

Para habilitar ou desabilitar uma região na organização

1. Entre no AWS Organizations console com as credenciais da conta de gerenciamento da sua organização.
2. Na página Contas da AWS, selecione a conta que você deseja atualizar.
3. Selecione a guia Configurações da conta.
4. Em Regiões, selecione a região que você deseja habilitar ou desabilitar.

5. Escolha Ações e, em seguida, escolha a opção Habilitar ou Desabilitar.
6. Se você tiver escolhido a opção Habilitar, analise o texto exibido e escolha Habilitar região.
7. Se você tiver escolhido a opção Desabilitar, analise o texto exibido, digite desabilitar para confirmar e, em seguida, escolha Desabilitar 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, é necessário ter a permissão que é mapeada 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 de ativação e desativação da região e conceder a outros a capacidade de ler e gravar.

O exemplo a seguir habilita uma região para a conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

Você também pode desabilitar uma região usando o mesmo comando e, depois, substituindo `enable-region` 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 de região em um determinado momento. Caso contrário, você receberá uma `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"
}
```

## Atualize o faturamento do seu Conta da AWS

Você pode atualizar todas as suas preferências de Conta da AWS cobrança usando o AWS Billing console Cost Management. Para saber como atualizar as configurações relacionadas ao faturamento da conta, consulte o [Guia do usuário do Gerenciamento de Faturamento e Custos da AWS](#):

## Atualize o endereço de e-mail do usuário-raiz

Há vários motivos comerciais pelos quais você pode precisar atualizar o endereço de e-mail do usuário-raiz para sua Conta da AWS. Por exemplo, segurança e resiliência administrativa. Este tópico explica o processo de atualização do endereço de e-mail do usuário-raiz para contas autônomas e de membros.

**Note**

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

Você pode atualizar o e-mail do usuário-raiz de forma diferente, dependendo se as contas são autônomas ou fazem parte de uma organização:

- Autônomo Contas da AWS — Se Contas da AWS não estiver associado a uma organização, você pode atualizar o e-mail do usuário raiz usando o AWS Management Console. Para saber como fazer isso, consulte [Update the root user email for a standalone Conta da AWS](#).
- Contas da AWS dentro de uma organização — Para contas membros que fazem parte de uma AWS organização, um usuário na conta de gerenciamento ou na conta de administrador delegado pode atualizar centralmente o e-mail do usuário raiz do conta membro a partir do AWS Organizations console ou programaticamente por meio da CLI & AWS SDKs Para saber como fazer isso, consulte [Atualizar o e-mail do usuário raiz para qualquer pessoa Conta da AWS em sua organização](#).

**Tópicos**

- [Atualize o e-mail do usuário raiz \(e-mail \) para uma conta autônoma Conta da AWS ou de gerenciamento](#)
- [Atualize o e-mail do usuário raiz \(e-mail \) para qualquer Conta da AWS pessoa em sua organização](#)

## Atualize o e-mail do usuário raiz (e-mail ) para uma conta autônoma Conta da AWS ou de gerenciamento

Para editar o endereço de e-mail do usuário raiz (endereço de autônomo Conta da AWS, execute as etapas no procedimento a seguir.

## Console de gerenciamento da AWS

### Note

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 [Console de gerenciamento da AWS](#) como 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 [Account](#), ao lado de Account details, escolha Actions e selecione Update email address and password.
4. Na página Account Details, ao lado de Email address, escolha Edit.
5. Na página Edit Account Email, preencha os campos New email address, Confirm new email address e confirme sua Password atual. Após, escolha Save and continue. Um código de verificação é enviado para o novo endereço de e-mail, de `no-reply@verify.signin.aws`.
6. Na página Edit Account Email, em Verification code, insira o código que você recebeu em seu e-mail e escolha Confirm updates.

### Note

Pode levar até cinco minutos para que o código de verificação chegue. Se você não vir a mensagem na caixa de entrada, verifique as pastas de spam e lixo eletrônico.

## AWS CLI & SDKs

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

## Atualize o e-mail do usuário raiz (e-mail ) para qualquer Conta da AWS pessoa em sua organização

Para editar o endereço de e-mail do usuário raiz (endereço de ) de qualquer conta membro em sua organização usando o AWS Organizations console, execute as etapas no procedimento a seguir.

### Note

Antes de atualizar o endereço de e-mail do usuário-raiz para uma conta de membro, recomendamos que você entenda o impacto dessa operação. Para obter mais informações, consulte [Updating the root user email address para uma conta de membro da AWS Organizations](#) no Guia do usuário do AWS Organizations .

Você também pode atualizar o endereço de e-mail do usuário raiz ( ) de uma [conta membro diretamente da página Conta](#) Console de gerenciamento da AWS após o login como usuário raiz. Para step-by-step obter instruções, siga as etapas fornecidas em [Atualize o e-mail do usuário raiz \(e-mail \) para uma conta autônoma Conta da AWS ou de gerenciamento](#).

### AWS Management Console


### Observações

- Para realizar este procedimento com a conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço Gerenciamento de conta](#).
- Você não pode usar este procedimento para acessar uma conta em uma organização diferente da que você está usando para chamar a operação.

Para atualizar o endereço de e-mail do usuário raiz, endereço de para uma conta de membro usando o AWS Organizations console

1. Faça login no [console do AWS Organizations](#). Você deve fazer login como um usuário do IAM ou fazer login como usuário-raiz ([não recomendado](#)) na conta gerencial da organização.
2. Na página Contas da AWS, escolha a conta de membro para a qual você deseja atualizar o endereço de e-mail do usuário-raiz.

3. Na seção Detalhes da conta, escolha o botão Ações e escolha Atualizar endereço de e-mail.
4. Em E-mail, insira o novo endereço de e-mail do usuário-raiz e escolha Salvar. Isso envia uma senha de uso único (OTP) para o novo endereço de e-mail.

 Note

Se precisar fechar esta página no console do Organizations enquanto espera pelo código, você pode retornar e concluir o processo de OTP dentro de 24 horas a partir do momento em que o código foi enviado. Para fazer isso, na página Detalhes da conta, escolha o botão Ações e, em seguida, escolha Concluir atualização por e-mail.

5. Em Código de verificação, insira o código que foi enviado para o novo endereço de e-mail na etapa anterior e escolha Confirmar. Isso confirma a atualização do usuário-raiz para a conta.

## AWS CLI & SDKs

Você pode recuperar ou atualizar o endereço de e-mail do usuário raiz (também chamado de endereço de e-mail principal) usando os seguintes AWS CLI comandos ou suas operações equivalentes no AWS SDK:

- [GetPrimaryEmail](#)
- [StartPrimaryEmailUpdate](#)
- [AcceptPrimaryEmailUpdate](#)

 Observações

- Para executar realizar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço de Gerenciamento 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:GetPrimaryEmail`
- `account:StartPrimaryEmailUpdate`
- `account:AcceptPrimaryEmailUpdate`

Se você usar essas permissões individuais, poderá conceder a alguns usuários a capacidade de ler somente as informações do endereço de e-mail do usuário-raiz e conceder a outros a capacidade de ler e gravar.

Para concluir o processo de endereço de e-mail do usuário raiz , você deve usar o e-mail principal em APIs conjunto na ordem em que são mostrados nos exemplos abaixo.

### Example **GetPrimaryEmail**

O exemplo a seguir recupera o endereço de e-mail do usuário-raiz da conta de membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account get-primary-email --account-id 123456789012
```

### Example **StartPrimaryEmailUpdate**

O exemplo a seguir inicia o processo de atualização do endereço de e-mail do usuário-raiz, identifica o novo endereço de e-mail e envia uma senha de uso único (OTP) para o novo endereço de e-mail da conta de membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email john@examplecorp.com
```

### Example **AcceptPrimaryEmailUpdate**

O exemplo a seguir aceita o código OTP e define o novo endereço de e-mail para a conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de Gerenciamento de Contas.

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678  
--primary-email john@examplecorp.com
```

## Atualizar senha do usuário-raiz

Para editar sua senha Conta da AWS de usuário root, execute as etapas no procedimento a seguir.

### Console de gerenciamento da AWS

#### Como editar sua senha de usuário-raiz

#### Note

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 [Console de gerenciamento da AWS](#) como 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 [Account](#), ao lado de Account details, escolha Actions e selecione Update email address and password.
4. Na página Account Details, ao lado de Password, escolha Edit.
5. Na página Edit password, preencha os campos Current password, New password e Confirm new password. Em seguida, selecione Update password. Para obter orientações adicionais, incluindo práticas recomendadas para definir senhas de usuário-raiz, consulte [Alterar a senha para o Usuário raiz da conta da AWS](#) no Guia do usuário do IAM.

### AWS CLI & SDKs

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

# Atualize seu Conta da AWS nome

Ao gerenciar várias Contas da AWS, use convenções de nomenclatura claras alinhadas com unidades de negócios e aplicativos para identificação e organização. Durante reorganizações, fusões, aquisições ou atualizações de convenções de nomenclatura, talvez seja necessário renomear contas para manter padrões administrativos e de identificação consistentes.

O nome de uma 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 dar nome às contas para poder dar nomes fáceis de reconhecer. Em contas corporativas, considere usar um padrão de nomenclatura, como organização-finalidade-ambiente (por exemplo, catálogo-de vendas-de produtos). Por motivos de privacidade e segurança, evite usar nomes de conta que reflitam informações de identificação pessoal (PII).

- **Independente Contas da AWS** — Se Contas da AWS não estiver associado a uma organização, você pode atualizar o nome da sua conta usando o Console de gerenciamento da AWS, ou o AWS CLI e. SDKs Para aprender a fazer isso, consulte [Atualize o nome da sua conta para uma conta autônoma Conta da AWS](#).
- **Contas da AWS dentro de uma organização** — Para contas de membros que fazem parte de uma AWS Organizations, um usuário na conta de gerenciamento ou na conta de administrador delegado pode atualizar centralmente o nome da conta de qualquer conta membro na organização a partir do AWS Organizations console ou programaticamente por meio do e. AWS CLI SDKs Para aprender a fazer isso, consulte [Atualize o nome da sua conta para qualquer Conta da AWS pessoa da sua organização](#).

## Note

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

## Tópicos

- [Atualize o nome da sua conta para uma conta autônoma Conta da AWS](#)
- [Atualize o nome da sua conta para qualquer Conta da AWS pessoa da sua organização](#)

## Atualize o nome da sua conta para uma conta autônoma Conta da AWS

Para alterar o nome da conta para uma conta autônoma Conta da AWS, execute as etapas no procedimento a seguir.

### Console de gerenciamento da AWS

#### Permissões mínimas

Você pode atualizar o nome da conta usando o usuário-raiz, um usuário do IAM ou um perfil do IAM. Se você estiver usando o usuário-raiz, nenhuma permissão adicional do IAM será necessária para atualizar o nome da conta. Ao usar um usuário ou perfil do IAM, você deve ter pelo menos as seguintes permissões do IAM:

- `account:GetAccountInformation`
- `account:PutAccountName`

Para atualizar o nome da conta de uma conta autônoma

1. Use seu endereço Conta da AWS de e-mail e senha para fazer login no [Console de gerenciamento da AWS](#) como 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 Detalhes da conta, escolha Ações e selecione Atualizar nome da conta.
4. Em Nome, insira o novo nome da conta que você deseja atualizar e escolha Salvar.

### AWS CLI & SDKs

#### Permissões mínimas

Você pode atualizar o nome da conta usando o usuário-raiz, um usuário do IAM ou um perfil do IAM. Para executar as etapas a seguir, seu usuário ou perfil do IAM deve ter, no mínimo, as seguintes permissões do IAM:

- `account:GetAccountInformation`

- `account:PutAccountName`

Para atualizar o nome da conta de uma conta autônoma

Você também pode usar uma das seguintes operações:

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
    --account-name "New-Account-Name"
```

- AWS SDKs: [PutAccountName](#)

## Atualize o nome da sua conta para qualquer Conta da AWS pessoa da sua organização

No modo AWS Organizations de todos os recursos, usuários autorizados do IAM ou funções do IAM nas contas de gerenciamento e de administrador delegado podem gerenciar centralmente os nomes das contas.

Para alterar o nome da conta de uma conta de membro de uma organização, execute as etapas mostradas no procedimento a seguir.

### Requisitos

Para atualizar o nome de uma conta com o AWS Organizations console, você precisa fazer algumas configurações preliminares:

- A organização precisa habilitar todos os atributos para gerenciar as configurações das contas de membros. Isso permite o controle administrativo das contas-membro. 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 atributos, consulte [Enabling all features for an organization](#).
- Você precisa habilitar o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulte [Habilite o acesso confiável para o gerenciamento de AWS contas](#).

## Console de gerenciamento da AWS

### Permissões mínimas

Para atualizar o nome da conta de uma conta de membro, seu usuário ou perfil do IAM deve ter as seguintes permissões:

- `organizations:DescribeOrganization` (somente console)
- `account:PutAccountName`

Para atualizar o nome da conta de uma conta de membro

1. Abra o console Organizations em <https://console.aws.amazon.com/organizations/>.
2. No painel de navegação à esquerda, selecione Contas da AWS.
3. Na página Contas da AWS, escolha a conta de membro que você deseja atualizar, escolha o menu suspenso Ações e escolha Atualizar nome da conta.
4. Em Nome, insira o nome atualizado e escolha Salvar.

## AWS CLI & SDKs

### Permissões mínimas

Para atualizar o nome da conta de uma conta de membro, seu usuário ou perfil do IAM deve ter as seguintes permissões:

- `organizations:DescribeOrganization` (somente console)
- `account:PutAccountName`

Para atualizar o nome da conta de uma conta de membro

Você também pode usar as seguintes operações:

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
    --account-id 111111111111 \  
    --account-name "New-Account-Name"
```

- AWS SDKs: [PutAccountName](#)

## 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 a receber todas as comunicações por e-mail enviadas para o e-mail da conta raiz.

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

- Contato de faturamento
- Contato de operações
- Contato de segurança

Você pode adicionar ou editar contatos alternativos de forma diferente, dependendo se as contas são autônomas 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 SDKs CLI &. Para saber como fazer isso, consulte [Update the alternate contacts for a standalone Conta da AWS](#).
- 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 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 SDKs Para saber como fazer isso, consulte [Atualizar os contatos alternativos para qualquer um Conta da AWS 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 prosseguir com a atualização das informações dos contatos alternativos da conta, recomendamos que você primeiro analise os requisitos a seguir quando 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 Console de gerenciamento da AWS procedimento abaixo sempre funciona somente no contexto autônomo. Você pode usar o Console de gerenciamento da AWS para acessar ou alterar somente os contatos alternativos na conta que você usou para chamar a operação.

### Console de gerenciamento da AWS

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 dos contatos alternativos)
- `account:PutAlternateContact` (para definir ou atualizar um contato alternativo)


- `account:DeleteAlternateContact` (para excluir um contato alternativo)

1. Faça login no [Console de gerenciamento da AWS](#) como um usuário ou perfil do IAM que tenha as permissões mínimas.
2. Escolha o nome da conta no canto superior direito da janela e depois escolha Conta.
3. Na página [Conta](#), role para baixo até Contatos alternativos e, à direita do título, escolha Editar.

 Note

Se você não vir a opção Editar, é provável que não tenha feito login como usuário-raiz da 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 executar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço Conta](#).

### Permissões mínimas

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

- `GetAlternateContact` (para ver os detalhes dos contatos 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 gravar.

## Example

O exemplo a seguir recupera o contato alternativo atual de faturamento 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 da 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, a primeira vez será bem-sucedida silenciosamente. Todas as tentativas posteriores geram uma exceção `ResourceNotFound`.

# 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:

- A organização precisa habilitar todos os atributos para gerenciar as configurações das contas de membros. Isso permite o controle administrativo das contas-membro. 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 atributos, consulte [Enabling all features for an organization](#).
- Você precisa habilitar o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulte [Habilite 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 o Gerenciamento de AWS contas para APIs que você possa acessar os dados da conta a partir do AWS Organizations console. Para ver as políticas gerenciadas atualizadas, consulte [Atualizações das políticas AWS gerenciadas da Organizations](#).

## Console de gerenciamento da AWS

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

1. Faça login no [console do AWS Organizations](#) com as credenciais da conta de gerenciamento da organização.
2. Em Contas da AWS, 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 executar realizar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço 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 dos contatos 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 gravar.

### Example

O exemplo a seguir recupera o contato alternativo de faturamento atual da conta do chamador de uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de 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 das operações da conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de 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 pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de 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, a primeira vez será bem-sucedida silenciosamente. Todas as tentativas posteriores geram uma exceção `ResourceNotFound`.

## conta: chave de `AlternateContactTypes` contexto

Você pode usar a chave de contexto `account:AlternateContactTypes` para especificar qual dos três tipos de faturamento é permitido (ou negado) pela política do IAM. O exemplo a seguir de

política de permissão do IAM usa essa chave de condição para permitir que as entidades principais anexadas recuperem, mas não modifiquem, somente o contato alternativo BILLING de uma conta específica em uma organização.

Como `account:AlternateContactTypes` é um tipo de string multivalor, você deve usar os operadores de string de vários valores [ForAnyValue](#) ou [ForAllValues](#).

## Atualize o contato principal do seu Conta da AWS

É possível atualizar as informações do contato principal associadas à conta, inclusive o nome completo do contato, o nome da empresa, o endereço de correspondência, o número de telefone e endereço do site.

Você pode editar o contato principal da conta de forma diferente, dependendo se as contas são autônomas 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 SDKs CLI &. Para saber como fazer isso, consulte [Atualizar contato Conta da AWS primário autônomo](#).
- **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 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 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](#)
- [Atualizar o contato principal de uma conta autônoma Conta da AWS ou de gerenciamento](#)
- [Atualize o contato principal de qualquer conta AWS membro em sua organização](#)

## Requisitos de número de telefone e endereço de e-mail

Antes de prosseguir com a atualização das informações do contato principal da conta, recomendamos que você primeiro analise os requisitos a seguir quando inserir números de telefone e endereços de e-mail.

- Os números de telefone só devem conter números.
- Os números de telefone devem começar com + e 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 não devem incluir espaços em branco entre o código de área, o código de troca e o código local. Por exemplo, +12025550179.
- Por motivos de segurança, os números de telefone devem ser capazes de receber SMS da AWS. Chamadas gratuitas não serão aceitas, pois a maioria não oferece suporte a SMS.
- 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. Configurar o [usuário-raiz](#) da conta com o endereço de e-mail ou o número de telefone de um indivíduo poderá dificultar a recuperação da conta se esse indivíduo deixar a empresa.

## Atualizar o contato principal de uma conta autônoma Conta da AWS ou de gerenciamento

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

### Console de gerenciamento da AWS

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 do contato principal)
- `account:PutContactInformation` (para atualizar os detalhes do contato principal)

1. Faça login no [Console de gerenciamento da AWS](#) como um usuário ou perfil do IAM que tenha as permissões mínimas.
2. Escolha o nome da conta no canto superior direito da janela e depois 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 executar realizar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço 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 gravar.

## Example

O exemplo a seguir recupera as informações do contato principal atual 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 as informações do novo contato principal da 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 conta AWS membro em sua organização

Para editar seus detalhes de contato principais em qualquer conta AWS membro em 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:

- A organização precisa habilitar todos os atributos para gerenciar as configurações das contas de membros. Isso permite o controle administrativo das contas-membro. 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 atributos, consulte [Enabling all features for an organization](#).
- Você precisa habilitar o acesso confiável para o serviço de gerenciamento de AWS contas. Para configurar isso, consulte [Habilite o acesso confiável para o gerenciamento de AWS contas](#).

## Console de gerenciamento da AWS

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

1. Faça login no [console do AWS Organizations](#) com as credenciais da conta de gerenciamento da organização.
2. Em Contas da AWS, selecione a conta que você deseja atualizar.
3. Escolha Informações de contato e localize Contato principal,
4. Selecione 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 executar essas operações na conta de gerenciamento ou em uma conta de administrador delegado em uma organização em relação a contas-membro, você precisa [habilitar o acesso confiável ao serviço 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 gravar.

### Example

O exemplo a seguir recupera as informações do contato principal atual da conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de 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 do contato principal da conta-membro especificada em uma organização. As credenciais usadas devem pertencer à conta de gerenciamento da organização ou à conta de administrador delegado do serviço de 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.

## 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 de forma exclusiva uma Conta da AWS. Muitos AWS recursos incluem o ID da conta em seus [nomes de recursos da Amazon \(ARNs\)](#). A parte do ID da conta distingue os recursos de uma conta dos recursos de outra conta. Se você for um usuário AWS Identity and Access Management (IAM), você pode entrar no Console de gerenciamento da AWS usando o ID da conta ou o alias da conta. Embora a conta IDs, como qualquer informação de identificação, deva ser usada e compartilhada com cuidado, ela não é considerada informação secreta, sensível ou confidencial.

### [ID de usuário canônico](#)

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 da Conta da AWS como o [usuário-raiz](#) ou um 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 Console de gerenciamento da AWS ou o AWS Command Line Interface (AWS CLI). No console, o local do ID da conta depende de você estar 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.

### Como encontrar o ID da conta como usuário-raiz

#### Console de gerenciamento da AWS

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:

- Quando você faz login como o usuário-raiz, não precisa de quaisquer permissões do IAM.

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

**i** Tip

Se você não vir a opção credenciais de segurança, significa que poderá ter feito login como usuário federado com um perfil do IAM, em vez de como usuário do IAM. Nesse caso, procure a conta de entrada e o número do ID da conta ao lado dela.

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

## AWS CLI & SDKs

Para encontrar seu Conta da AWS ID usando o AWS CLI

**i** Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- Quando você executa o comando como o usuário-raiz, não precisa de quaisquer permissões do IAM.

Use o comando [get-caller-identity](#) da seguinte forma.

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

## Encontrar o ID da conta como usuário do IAM

### Console de gerenciamento da AWS

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

**i** Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- `account:GetAccountInformation`

1. No canto superior direito da barra de navegação, escolha seu nome de usuário e selecione Credenciais de segurança.

 Tip

Se você não vir a opção credenciais de segurança, significa que poderá ter feito login como usuário federado com um perfil do IAM, em vez de como usuário do IAM. Nesse caso, procure a conta de entrada e o número do ID da conta ao lado dela.

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

## 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:

- Quando executa o comando como usuário ou perfil 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 Console de gerenciamento da AWS ou o AWS CLI O 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.

## Encontrar o ID de usuário canônico como o usuário-raiz ou um usuário do IAM

### Console de gerenciamento da AWS

Para encontrar o ID de usuário canônico da conta quando você tiver feito login no console como usuário-raiz ou um usuário do IAM

#### Permissões mínimas

Para executar as etapas a seguir, é necessário ter as seguintes permissões do IAM:

- Quando você executa o comando como o usuário-raiz, não precisa de quaisquer permissões do IAM.
- Quando fizer login como usuário do IAM, você deverá ter:
  - `account:GetAccountInformation`

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

#### Tip

Se você não vir a opção credenciais de segurança, significa que poderá ter feito login como usuário federado com um perfil do IAM, em vez de como usuário do IAM. Nesse caso, procure a conta de entrada e o número do ID da conta ao lado dela.

3. Na seção Detalhes da conta, o ID de usuário canônico aparece ao lado de ID de usuário canônico. Você pode usar seu ID de usuário canônico para configurar as listas de controle de acesso do Amazon S3 ([https://docs.aws.amazon.com/AmazonS3/latest/dev/AccessControl.html](#)). ACLs

### AWS CLI & SDKs

Para encontrar o ID de usuário canônico usando o AWS CLI

O mesmo comando AWS CLI e o comando da API funcionam para Usuário raiz da conta da AWS os usuários do IAM ou para as funções do IAM.

Use o comando [list-buckets](#) como a seguir.

```
$ aws s3api list-buckets \  
  --max-items 10 \  
  --page-size 10 \  
  --query Owner.ID \  
  --output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

## Encontrar o ID canônico como um usuário federado com um perfil do IAM

### Console de gerenciamento da AWS

Para encontrar o ID de usuário canônico da conta quando você tiver feito login no console como usuário federado com um perfil do IAM

#### Permissões mínimas

- Você deve ter permissão para listar e visualizar um bucket do Amazon S3.

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

### AWS CLI & SDKs

Para encontrar o ID de usuário canônico usando o AWS CLI

O mesmo comando AWS CLI e o comando da API funcionam para Usuário raiz da conta da AWS os usuários do IAM ou para as funções do IAM.

Use o comando [list-buckets](#) como a seguir.

```
$ aws s3api list-buckets \  
  --max-items 10 \  
  --page-size 10 \  
  --query Owner.ID \  
  --output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

```
--max-items 10 \  
--page-size 10 \  
--query Owner.ID \  
--output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

# Segurança no gerenciamento de AWS contas

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

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

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao gerenciamento de contas, consulte [Serviços da AWS escopo por programa de conformidade Serviços da AWS](#) .
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço 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

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Gerenciamento de AWS Contas. Ela mostra como configurar o Gerenciamento de Contas para atender aos objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos de gerenciamento de contas.

## Tópicos

- [Proteção de dados no gerenciamento de AWS contas](#)
- [AWS PrivateLink para gerenciamento de AWS contas](#)
- [Identity and Access Management para gerenciamento de AWS contas](#)
- [AWS políticas gerenciadas para gerenciamento de AWS contas](#)
- [Validação de conformidade para gerenciamento de AWS contas](#)
- [Resiliência no gerenciamento de AWS contas](#)
- [Segurança da infraestrutura em AWS Gerenciamento de contas](#)

## 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 o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para saber mais sobre a privacidade de dados, consulte as [Data Privacy FAQ](#). Para saber mais sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and RGPD](#) no Blog de segurança da AWS .

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

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como [trabalhar com CloudTrail trilhas](#) no Guia AWS CloudTrail do usuário.
- 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 sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Gerenciamento de Contas ou outros Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em

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 fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

## AWS PrivateLink para gerenciamento de AWS contas

Se você usa a Amazon Virtual Private Cloud (Amazon VPC) para hospedar seus AWS recursos, você pode acessar o serviço de gerenciamento de AWS contas de dentro da VPC sem precisar cruzar a Internet pública.

A Amazon VPC permite que você lance AWS recursos 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 mais informações sobre VPCs, consulte o Guia do [usuário da Amazon VPC](#).

Para conectar a Amazon VPC ao Gerenciamento de Contas, primeiro você deve definir um endpoint da VPC de interface, que permite conectar a VPC a outros produtos da AWS. 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

Você pode criar um endpoint de gerenciamento de AWS contas em sua VPC usando Console de gerenciamento da AWS o, AWS Command Line Interface the AWS CLI(), AWS um SDK, AWS a API de gerenciamento de contas ou. CloudFormation

Para obter informações sobre como criar e configurar um endpoint usando o console da Amazon VPC ou o AWS CLI, consulte [Criação de um endpoint de interface](#) no Guia do usuário da Amazon VPC.

#### Note

Ao criar um endpoint, especifique o Gerenciamento de Contas como o serviço ao qual a VPC deve se conectar, usando o seguinte formato:

```
com.amazonaws.us-east-1.account
```

Você deve usar a string exatamente como mostrada, especificando a região us-east-1. Como um serviço global, o gerenciamento de contas é hospedado somente nessa AWS região.

Para obter informações sobre como criar e configurar um endpoint usando CloudFormation, consulte o VPC endpoint recurso [AWS: :EC2::](#) no Guia do usuário.CloudFormation

## Políticas de endpoint da Amazon VPC

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

- [Políticas de endpoint da Amazon Virtual Private Cloud para o Gerenciamento de Contas](#)
- [Controle do acesso a serviços com endpoints da VPC](#) no Guia do AWS PrivateLink .

## Políticas de endpoint da Amazon Virtual Private Cloud para o Gerenciamento de Contas

Você pode criar uma política de endpoint da Amazon VPC para o Gerenciamento de Contas, na qual você especifica o seguinte:

- A entidade principal que pode realizar ações.
- As ações que as entidades principais podem executar.
- Os recursos nos quais as ações podem ser executadas.

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

Se você quiser conceder acesso às contas que fazem parte de uma AWS organização a um principal que esteja em uma das contas membros da organização, o Resource elemento deverá usar o seguinte formato:

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

Para obter mais informações sobre a criação de políticas de endpoint, consulte [Controle do acesso a serviços com endpoints da VPC](#) no Guia do AWS PrivateLink .

## Identity and Access Management para gerenciamento de AWS contas

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

### Tópicos

- [Público](#)
- [Autenticação com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como o gerenciamento de AWS contas funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS](#)
- [Usando políticas baseadas em identidade \(políticas do IAM\) 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 com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte [Solução de problemas de identidade e acesso ao gerenciamento de AWS contas](#)).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte [Como o gerenciamento de AWS contas funciona com o IAM](#))
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte [Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS](#))

## Autenticação com identidades

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

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como AWS IAM Identity Center (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte [Como fazer login em sua Conta da AWS](#) no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte [AWS Signature Version 4 para solicitações de API](#) no Guia do usuário do IAM.

### Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em [Tarefas que exigem credenciais de usuário-raiz](#) no Guia do usuário do IAM.

### Identidade federada

Como prática recomendada, exija que os usuários humanos 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 corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos AWS IAM Identity Center. Para saber mais, consulte [O que é o IAM Identity Center?](#) no Guia do usuário do AWS IAM Identity Center .

### Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte [Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias](#) no Guia do usuário do IAM.

Um [grupo do IAM](#) especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte [Casos de uso de usuários do IAM](#) no Guia do usuário do IAM.

## Perfis do IAM

Uma [perfil do IAM](#) é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função [mudando de um usuário para uma função do IAM \(console\)](#) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte [Métodos para assumir um perfil](#) no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte [Visão geral das políticas JSON](#) no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

## Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades).

Para saber como escolher entre uma política gerenciada e políticas em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

## Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário [especificar uma entidade principal](#) em uma política baseada em recursos.

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

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte [Políticas de controle de serviço](#) no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte [Políticas de controle de recursos \(RCPs\)](#) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte [Políticas de sessão](#) no Guia do usuário do IAM.

## Vários tipos de política

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

## Como o gerenciamento de AWS contas funciona com o IAM

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

Recursos do IAM que você pode usar com o gerenciamento de AWS contas

Recurso do IAM	Suporte ao Gerenciamento de Contas
<a href="#">Políticas baseadas em identidade</a>	Sim
<a href="#">Políticas baseadas em recurso</a>	Não
<a href="#">Ações de políticas</a>	Sim
<a href="#">Recursos de políticas</a>	Sim
<a href="#">Chaves de condição de políticas</a>	Sim
<a href="#">ACLs</a>	Não
<a href="#">ABAC (tags em políticas)</a>	Não
<a href="#">Credenciais temporárias</a>	Sim
<a href="#">Permissões de entidade principal</a>	Sim
<a href="#">Perfis de serviço</a>	Não
<a href="#">Funções vinculadas ao serviço</a>	Não

Para ter uma visão de alto nível de como o gerenciamento de contas e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

### Políticas baseadas em identidade para Gerenciamento de Contas

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. 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 [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte [Referência de elemento de política JSON do IAM](#) no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para o Gerenciamento de Contas

Para visualizar 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

Compatibilidade com políticas baseadas em recursos: não

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

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Ações de política para Gerenciamento de Contas

Compatível com ações de políticas: sim

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

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. 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 prefixo a seguir 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 visualizar 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 políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Para ações que não oferecem compatibilidade com permissões em nível de recurso, 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 em um `Resources` elemento de política do IAM para ajudar você a filtrar a política e distinguir entre esses tipos de Contas da AWS:

- `account`

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

- `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 seus ARNs, consulte [Recursos definidos pelo gerenciamento de AWS contas](#) na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pelo gerenciamento de AWS contas](#).

Para visualizar 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 Gerenciamento de Contas

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

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

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. 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. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

O serviço de Gerenciamento de Contas oferece suporte às seguintes chaves de condição que você pode usar para fornecer filtragem refinada para as políticas do IAM:

- `conta: TargetRegion`

Essa chave de condição usa um argumento que consiste em uma lista de [códigos de região da AWS](#). Ela permite filtrar 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 direcionadas aos tipos de contato alternativos especificados.

- conta: AccountResourceOrgPaths

Essa chave de condição usa um argumento que consiste em uma lista de caminhos na hierarquia de sua organização para unidades organizacionais (UO) específicas. Ela permite que você filtre a política para afetar somente contas de destino em uma UO correspondente.

```
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. Ela permite que você filtre 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.

- conta: EmailTargetDomain

Essa chave de condição usa um argumento que consiste em uma lista de domínios de e-mail. Ela permite filtrar a política para afetar somente as ações que correspondem aos domínios de e-mail especificados. Essa chave de condição diferencia maiúsculas de minúsculas. Você deve usar `StringEqualsIgnoreCase` em vez de `StringEquals` no bloco de condição da política para controlar a ação com base no domínio do endereço de e-mail de destino. Aqui está um exemplo de política que permite que a ação `account:StartPrimaryEmailUpdate` seja concluída quando o domínio de e-mail contém `example.com`, `company.org` ou qualquer combinação de maiúsculas e minúsculas, como `EXAMPLE.COM`.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowConditionKey",
    "Effect": "Allow",
    "Action": [
      "account:StartPrimaryEmailUpdate"
    ],
    "Resource": "*",
    "Condition": {
      "StringEqualsIgnoreCase": {
        "account:EmailTargetDomain": [
          "example.com",
          "company.org"
        ]
      }
    }
  }
]
```

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 visualizar 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 em Gerenciamento de Contas

### Suportes ACLs: Não

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

## Controle de acesso por atributo com o Gerenciamento de Contas

Oferece compatibilidade com ABAC (tags em políticas): não

O controle de acesso por atributo (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 entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para o gerenciamento de AWS contas, o controle de acesso baseado em tags é suportado somente por meio da chave de `account:AccountResourceOrgTags/key-name` condição. A chave de `aws:ResourceTag/key-name` condição padrão não é suportada APIs no namespace da conta.

Exemplo de política JSON usando a chave de condição compatível

O exemplo de política a seguir permite acessar as informações de contato de contas marcadas com a chave "CostCenter" e o valor "12345" ou "67890" em sua organização.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "account:GetContactInformation",
        "account:GetAlternateContact"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "account:AccountResourceOrgTags/CostCenter": [
            "12345",
            "67890"
          ]
        }
      }
    }
  ]
}
```

Para obter mais informações sobre o ABAC, consulte [Definir permissões com base em atributos com autorização ABAC](#) e o [tutorial do IAM: Definir permissões para acessar AWS recursos com base em tags no Guia](#) do usuário do IAM.

## Usar credenciais temporárias com o Gerenciamento de Contas

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte [Credenciais de segurança temporárias no IAM](#) e [Serviços da Serviços da AWS que funcionam com o IAM](#) no Guia do usuário do IAM.

## Permissões de entidade principal entre serviços para o Gerenciamento de Contas

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Sessões de acesso direto](#).

## Perfis de serviço para o Gerenciamento de Contas

Compatível com perfis de serviço: não

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

## Perfis vinculados a serviços para o 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. AWS service (Serviço da AWS) O serviço pode assumir o perfil 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

administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte [Serviços da AWS que funcionam com o IAM](#). Encontre um serviço na tabela que inclua um Yes na coluna Perfil vinculado 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 perfis não têm permissão para criar ou modificar recursos do Gerenciamento de Contas. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte [Criar políticas do IAM \(console\)](#) no Guia do usuário do IAM.

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

- [Práticas recomendadas de política](#)
- [Usando a página Conta no Console de gerenciamento da AWS](#)
- [Fornecendo acesso somente para leitura à página Conta no Console de gerenciamento da AWS](#)
- [Fornecendo acesso total à página Conta no Console de gerenciamento da AWS](#)

### Práticas recomendadas de política

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

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões

definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte [Elementos da política JSON do IAM: condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

## Usando a página Conta no Console de gerenciamento da AWS

Para acessar a [página Conta](#) no Console de gerenciamento da AWS, 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 que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis do IAM) 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 saber mais, consulte [Adicionar permissões a um usuário](#) no Guia do usuário do IAM.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a AWS CLI ou a AWS API. Em vez disso, em muitos casos você poderá optar por permitir o acesso somente às ações que corresponderem às operações da API que você estiver tentando executar.

## Fornecendo acesso somente para leitura à página Conta no Console de gerenciamento da AWS

No exemplo a seguir, você deseja conceder a um usuário do IAM na Conta da AWS acesso somente leitura à página Conta no Console de gerenciamento da AWS. Usuários com essa política anexada não podem fazer qualquer alteração.

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

### JSON

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

## Fornecendo acesso total à página Conta no Console de gerenciamento da AWS

No exemplo a seguir, você deseja conceder a um usuário do IAM na Conta da AWS acesso total à página Conta no Console de gerenciamento da AWS. 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`

JSON

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

## Usando políticas baseadas em identidade (políticas do IAM) para AWS gerenciamento de contas

Para uma discussão completa sobre usuários Contas da AWS e usuários do IAM, consulte [O que é o IAM?](#) no Guia do usuário do IAM.

Para obter instruções sobre como atualizar as políticas gerenciadas pelo cliente, consulte [Editar políticas do IAM](#) no Guia do usuário do IAM.


## AWS Políticas de ações de gerenciamento de contas

Esta tabela resume as permissões que concedem acesso às configurações da conta. Para obter exemplos de políticas que usam essas permissões, consulte [Exemplos de políticas baseadas em identidade para gerenciamento de contas AWS](#).

### Note

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

Nome da permissão	Nível de acesso	Description
<code>account:ListRegions</code>	Lista	Concede permissão para listar as regiões disponíveis.
<code>account:GetAccountInformation</code>	Ler	Concede permissão para recuperar as informações de uma conta.
<code>account:GetAlternateContact</code>	Ler	Concede permissão para recuperar os contatos alternativos de uma conta.
<code>account:GetContactInformation</code>	Ler	Concede permissão para recuperar as informações do contato principal de uma conta.
<code>account:GetPrimaryEmail</code>	Ler	Concede permissão para recuperar o endereço de e-mail principal de uma conta.

Nome da permissão	Nível de acesso	Description
<code>account:GetRegionOptStatus</code>	Ler	Concede permissão para obter o status de ativação de uma região.
<code>account:AcceptPrimaryEmailUpdate</code>	Gravar	Concede permissão para aceitar a atualização do endereço de e-mail principal da conta do membro em uma AWS organização.
<code>account:CloseAccount</code>	Gravar	Concede permissão para fechar uma conta. <div data-bbox="1068 800 1511 1209" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Esta é uma permissão somente para o console. Não há acesso de API disponível para esta permissão.</p> </div>
<code>account&gt;DeleteAlternateContact</code>	Gravar	Concede permissão para excluir os contatos alternativos de uma conta.
<code>account:DisableRegion</code>	Gravar	Concede permissão para desabilitar o uso de uma região.
<code>account:EnableRegion</code>	Gravar	Concede permissão para habilitar o uso de uma região.
<code>account:PutAccountName</code>	Gravar	Concede permissão para atualizar o nome de um conta.

Nome da permissão	Nível de acesso	Description
<code>account:PutAlternateContact</code>	Gravar	Concede permissão para modificar os contatos alternativos de uma conta.
<code>account:PutContactInformation</code>	Gravar	Concede permissão para atualizar as informações do contato principal de uma conta.
<code>account:StartPrimaryEmailUpdate</code>	Gravar	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 ajudar no diagnóstico e na correção de problemas comuns que você pode encontrar quando trabalhar com o Gerenciamento de Contas e o IAM.

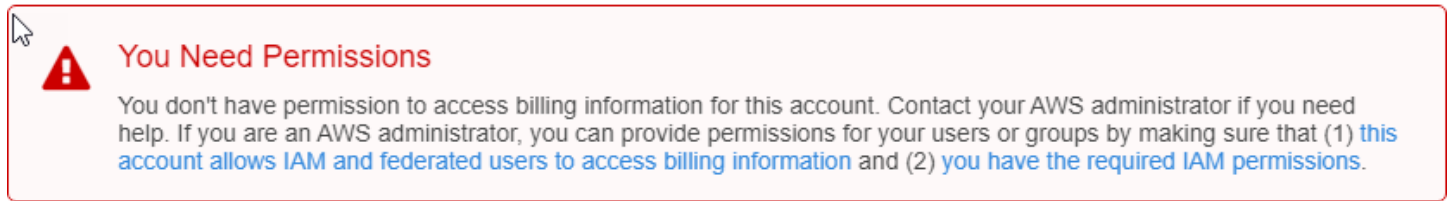
### Tópicos

- [Não tenho autorização para executar uma ação na página Contas](#)
- [Não estou autorizado a executar iam:PassRole](#)
- [Quero permitir que pessoas fora da minha acessem Conta da AWS os detalhes da minha conta](#)

### Não tenho autorização para executar uma ação na página Contas

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

O exemplo de erro a seguir ocorre quando o usuário do mateojackson IAM tenta usar o console para ver detalhes sobre ele Conta da AWS na página Conta do Console de gerenciamento da AWS , 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 uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as políticas deverão ser atualizadas para permitir a passagem de um perfil 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 uma usuária do IAM chamada `marymajor` tenta usar o console para executar 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

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível 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 é compatível com esses recursos, consulte [Como o gerenciamento de AWS contas funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como [fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## AWS políticas gerenciadas para gerenciamento de AWS contas

AWS Atualmente, o Gerenciamento de Contas fornece duas políticas AWS gerenciadas que estão disponíveis para seu uso:

- [AWS política gerenciada: AWSAccount ManagementReadOnlyAccess](#)
- [AWS política gerenciada: AWSAccount ManagementFullAccess](#)
- [Atualizações do gerenciamento de contas nas políticas AWS gerenciadas](#)

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as [políticas gerenciadas pelo cliente](#) que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para saber mais, consulte [AWS Políticas gerenciadas pela](#) no Guia do usuário do IAM.

## AWS política gerenciada: AWSAccountManagementReadOnlyAccess

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

Essa política fornece permissões somente leitura para a visualização apenas do seguinte:

- Os metadados sobre o seu Contas da AWS
- Os Regiões da AWS que estão ativados ou desativados para o Conta da AWS (você pode ver o status das regiões em sua conta somente usando o AWS console)

Ele faz isso concedendo permissão para executar qualquer uma das operações `Get*` ou `List*`. Ele não fornece nenhuma capacidade de modificar os metadados da conta ou ativar ou desativar Regiões da AWS a conta.

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- `account`— Permite que os diretores recuperem as informações de metadados sobre. Contas da AWS Também permite que as entidades principais listem as Regiões da AWS que estão habilitadas para a conta no Console de gerenciamento da AWS.

### JSON

```
{
```

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

## AWS política gerenciada: AWSAccount ManagementFullAccess

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

Essa política fornece acesso administrativo total para a visualização ou a modificação do seguinte:

- Os metadados sobre o seu Contas da AWS
- As Regiões da AWS que estão ativadas ou desativadas para o Conta da AWS (você pode ver o status ou ativar ou desativar regiões da sua conta somente usando o AWS console)

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

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- `account`— permite que os diretores visualizem ou modifiquem as informações de metadados sobre. Contas da AWS Também permite que as entidades principais listem as Regiões da AWS que estão habilitadas para a conta e as habilitem ou desabilitem no Console de gerenciamento da AWS.

### JSON

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

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

## Atualizações do gerenciamento de contas nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas de gerenciamento de contas desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nesta página, assine o feed de RSS na página Histórico do documento do Gerenciamento de Contas.

Alteração	Descrição	Data
AWS O gerenciamento de contas foi lançado com novas políticas AWS gerenciadas e começou a monitorar as mudanças	O gerenciamento de contas foi lançado inicialmente com as seguintes políticas AWS gerenciadas: <ul style="list-style-type: none"><li>• <a href="#">AWSAccountManagementReadOnlyAccess</a></li><li>• <a href="#">AWSAccountManagementFullAccess</a></li></ul>	30 de setembro de 2021

## Validação de conformidade para gerenciamento de AWS contas


Audidores 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 AWS escopo por programa de conformidade Serviços da AWS](#) . Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) Guia do AWS Artifact usuário.

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

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- [Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

 Note

Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a [Referência dos serviços qualificados pela HIPAA](#).

- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub CSPM](#)— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.
- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

## Resiliência no gerenciamento de AWS contas

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente

executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

## Segurança da infraestrutura em AWS Gerenciamento de contas

Como serviços gerenciados, AWS os serviços executados em seu Conta da AWS são protegidos pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar as configurações da conta pela rede. Os clientes devem oferecer compatibilidade com:

- 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.

# Monitore sua Conta da AWS

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. AWS fornece as seguintes ferramentas de monitoramento para monitorar o gerenciamento de contas, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- AWS CloudTrail captura (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 que você identifique quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).
- EventBridge da 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 determinar 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](#).

## Registrando chamadas da API de gerenciamento de AWS contas usando AWS CloudTrail

O gerenciamento de AWS contas APIs é integrado com AWS CloudTrail um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço que chama uma operação de gerenciamento de contas. CloudTrail captura todas as chamadas da API de gerenciamento de contas como eventos. As chamadas capturadas incluem todas as chamadas para as operações do Gerenciamento de Contas. Se você criar uma trilha, poderá ativar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para operações de gerenciamento de contas. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que 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 isso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

## Informações de gerenciamento de contas em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre com uma operação de gerenciamento de contas, CloudTrail registra essa atividade em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo de eventos em sua empresa Conta da AWS, incluindo eventos para operações de gerenciamento de contas, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no Console de gerenciamento da AWS, a trilha se aplica a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

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

AWS CloudTrail registra todas as operações da API de gerenciamento de contas encontradas na seção [Referência da API](#) deste guia. Por exemplo, chamadas para as `PutAlternateContact` operações `CreateAccountDeleteAlternateContact`, e geram entradas nos arquivos de CloudTrail log.

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

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (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 AWS serviço

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

## Noções básicas das entradas de log do Gerenciamento de Contas

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

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

### Example Exemplo 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "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 CloudTrail registro de uma chamada para a PutAlternateContact operação para adicionar um novo contato BILLING alternativo a uma conta.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO1234567890EXAMPLE",
        "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 CloudTrail registro para uma chamada para a `DeleteAlternateContact` operação para excluir o contato OPERATIONS alternativo atual.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO0A1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO0A1234567890EXAMPLE",
        "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 do Gerenciamento de Contas

Os exemplos a seguir mostram eventos do Gerenciamento de Contas. Os eventos são emitidos com base no melhor esforço.

Atualmente, somente eventos específicos para ativar e desativar regiões e chamadas de API CloudTrail estão disponíveis para o gerenciamento de contas.

## Tipos de eventos

- [Evento para habilitar e desabilitar regiões](#)

## Evento para habilitar e desabilitar regiões

Quando você habilita ou desabilita uma região em uma conta, 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, em 2020-09-30, a região ap-east-1 foi ENABLED para a 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 pelo GetRegionOptStatus e ListRegions APIs

- ENABLED: a região foi habilitada com êxito para o accountId indicado
- ENABLING: a região está em processo de habilitação para o accountId indicado
- DISABLED: a região foi desabilitada com êxito para o accountId indicado

- **DISABLING:** a região está em processo de desabilitação 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 os eventos **ENABLED** e **DISABLED** da região.

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

# Solucione problemas do seu Conta da AWS

Use as informações dos tópicos a seguir para ajudar no diagnóstico e na correção de problemas com a Conta da AWS. Para obter ajuda com o usuário-raiz, consulte [Solucionar problemas com o usuário-raiz](#) no Guia do usuário do IAM. Para obter ajuda com o processo de login, consulte [Solução de problemas de login da Conta da AWS](#) no Manual do usuário fazer login da AWS .

## Tópicos de solução de problemas

- [Solução de problemas com a Conta da AWS criação](#)
- [Solução de problemas com o Conta da AWS fechamento](#)
- [Solucionando outros problemas com Contas 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	Fonte
Não sei como me cadastrar ou criar uma conta	<a href="#">Crie um Conta da AWS</a>	Este guia
O que devo fazer se eu não receber uma ligação AWS para verificar minha nova conta ou se o PIN que eu inseri não funciona?	<a href="https://repost.aws/knowledge-center/phone-verify-no-call">https://repost.aws/knowledge-center/phone-verify-no-call</a>	AWS re:Post
Como resolvo o erro “número máximo de tentativas malsucedidas” quando tento verificar minhas Conta da AWS por telefone?	<a href="https://repost.aws/knowledge-center/maximum-tentativas-fracassadas">https://repost.aws/knowledge-center/maximum-tentativas-fracassadas</a>	AWS re:Post

Problema	Link de referência	Fonte
Já se passaram mais de 24 horas e minha conta não está ativada	<a href="https://repost.aws/knowledge-center/create-and-activate-aws-account">https://repost.aws/knowledge-center/create-and-activate-aws-account</a>	AWS re:Post
Não consigo fazer login na nova conta depois que ela foi criada	<a href="https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html">https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html</a>	AWS Guia do usuário de login

Para obter ajuda adicional, recomendamos que você pesquise o [AWS re:Post](#) para conhecer o conteúdo relacionado ao seu problema específico. Se você ainda precisar de assistência, entre em contato com o [AWS Support](#).

## Solução de problemas com o Conta da AWS fechamento

Use as informações abaixo para obter ajuda no diagnóstico e na correção de problemas comuns encontrados durante o processo de encerramento da conta. Para obter informações gerais sobre o processo de encerramento da conta, consulte [Fechar um Conta da AWS](#).

### Tópicos

- [Não sei como excluir ou cancelar a conta](#)
- [Não vejo o botão Encerrar conta na página Contas](#)
- [Encerrei minha conta, mas ainda não recebi uma confirmação por e-mail](#)
- [Eu recebo um erro ConstraintViolationException "" ao tentar fechar minha conta](#)
- [Recebo o erro "CLOSE\\_ACCOUNT\\_QUOTA\\_EXCEEDED" ao tentar encerrar uma conta-membro](#)
- [Preciso excluir minha AWS organização antes de fechar a conta de gerenciamento?](#)

### Não sei como excluir ou cancelar a conta

Para encerrar a conta, siga as instruções em [Fechar um Conta da AWS](#).

## Não vejo o botão Encerrar conta na página Contas

Se sua conexão não for como usuário-raiz, o botão Encerrar conta não será exibido na página Contas. Você deve [fazer login Console de gerenciamento da AWS como usuário root](#) para fechar sua conta. Se você não conseguir fazer login, consulte [Solucionar problemas com o usuário-raiz](#).

## Encerrei minha conta, mas ainda não recebi uma confirmação por e-mail

Essa confirmação por e-mail só é enviada ao endereço de e-mail do usuário-raiz para sua Conta da AWS. Se você não receber esse e-mail em algumas horas, poderá fazer [login no Console de gerenciamento da AWS como usuário root](#) para verificar se sua conta foi encerrada. Se a conta tiver sido encerrada com êxito, será exibida uma mensagem indicando que a 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 CLOSED no AWS Organizations console. Para obter mais informações, consulte [Fechar uma conta-membro na sua organização](#) no Guia do usuário do AWS Organizations .

Se você estiver tentando encerrar uma conta de gerenciamento e não receber uma confirmação por e-mail sobre o encerramento da conta, provavelmente a organização tem contas-membro ativas. Você só poderá encerrar a conta de gerenciamento se a organização não tiver contas-membro ativas. 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 Closed lado dos nomes das contas. Depois disso, você pode encerrar 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 Console de gerenciamento da AWS como usuário root da](#) conta de gerenciamento e fechá-la na página Contas. Para obter mais informações, consulte [Closing a management account in your organization](#) no AWS Organizations User Guide.

## Recebo o erro "CLOSE\_ACCOUNT\_QUOTA\_EXCEEDED" ao tentar encerrar uma conta-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 encerramento mínimo de contas é dez e o encerramento máximo de contas é mil, mesmo que 10% das contas exceda mil. Para obter mais informações sobre cotas do Organizations, consulte [Quotas for AWS Organizations](#) no AWS Organizations User Guide.

## 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. Entretanto, você só poderá encerrar a conta de gerenciamento se a organização não tiver contas-membro ativas. 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 Closed lado dos nomes das contas. Depois disso, você pode encerrar a conta de gerenciamento.

## Solucionando outros problemas com Contas da AWS

Use as informações aqui contidas para obter ajuda para solucionar problemas relacionados à Conta da AWS.

### Problemas

- [Preciso trocar o cartão de crédito do meu Conta da AWS](#)
- [Preciso denunciar atividades fraudulentas Conta da AWS](#)
- [Eu preciso fechar meu Conta da AWS](#)

## Preciso trocar o cartão de crédito do meu Conta da AWS

Para alterar o cartão de crédito do seu Conta da AWS, você deve conseguir fazer login. AWS tem proteções em vigor que exigem que você prove que é o proprietário da conta. Para obter instruções, consulte [Gerenciar métodos de pagamento de cartão de crédito](#) no Guia do usuário do AWS Billing .

## Preciso denunciar atividades fraudulentas Conta da AWS

Se você suspeitar de atividade fraudulenta usando o seu Conta da AWS e quiser fazer uma denúncia, consulte [Como faço para denunciar o abuso de AWS recursos](#).

Se você estiver tendo problemas com uma compra feita na Amazon.com, consulte o [Serviço de atendimento ao cliente da Amazon](#).

## Eu preciso fechar meu Conta da AWS

Para obter ajuda na solução de problemas com o fechamento do seu Conta da AWS, consulte [Fechar um Conta da AWS](#).

# 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 do encerramento da conta, você pode reabri-la até 90 dias a partir do dia do encerramento da conta. O intervalo de tempo entre o dia do encerramento da conta e o encerramento permanente da conta pela AWS é denominado [período pós-encerramento](#).

## O que você precisa saber antes de encerrar a conta

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

- O encerramento da conta servirá como seu aviso de rescisão do Contrato de Cliente da AWS para esta 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 [documentação da AWS](#) apropriada desse serviço.
- Você pode reabrir a conta durante o período [pós-encerramento](#). As cobranças pelos serviços que permaneceram na conta serão reiniciadas se você reabri-la. Você também permanece responsável por quaisquer faturas não pagas e por [Instâncias Reservadas](#) e [Savings Plans](#) pendentes.
- Você permanece responsável por todas as taxas e cobranças 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 tiver fechado a conta em 15 de janeiro, receberá uma fatura no início de fevereiro pelo uso incorrido de 1.º de janeiro a 15 de janeiro. Você continuará recebendo faturas de [instâncias reservadas](#) e de [Savings Plans](#) depois de encerrar a conta até que eles expirem.
- Você não poderá mais acessar os AWS serviços que estavam disponíveis anteriormente em sua conta. No entanto, você poderá fazer login e acessar uma Conta da AWS encerrada durante o [período pós-encerramento](#) apenas para ver informações anteriores de faturamento, acessar as configurações da conta ou entrar em contato com o [AWS Support](#).
- Não é possível usar o mesmo endereço de e-mail registrado na Conta da AWS no momento do encerramento como e-mail principal de outra Conta da AWS. Se você quiser usar o mesmo endereço de e-mail para uma Conta da AWS diferente, recomendamos atualizá-lo antes do

encerramento. Para obter mais informações, consulte [Atualize o endereço de e-mail do usuário-raiz](#).

- Se você tiver [habilitado autenticação multifator \(MFA\)](#) no usuário-raiz da Conta da AWS ou tiver configurado o [dispositivo com MFA em um usuário do IAM](#), a MFA não será removida automaticamente quando você encerrar a conta. Se você optar por deixar a MFA ativada durante o [período pós-encerramento](#) de 90 dias, mantenha o dispositivo com MFA ativo até que o período pós-encerramento expire, caso você precise acessar a conta durante esse período. Observe que os dispositivos token TOTP de hardware não podem ser associados a outro usuário após o encerramento permanente da conta. Se você quiser usar o token TOTP de hardware com outro usuário posteriormente, terá a opção de [desativar o dispositivo com MFA de hardware](#) antes de encerrar a conta. Os dispositivos com MFA para [usuários do IAM](#) devem ser excluídos pelo administrador da conta.

### Considerações adicionais para contas-membro

- Quando uma conta-membro for encerrada, ela só será removida da organização 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 considerada na cota, consulte [Remove a member account from your organization](#) antes de encerrá-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 encerramento mínimo de contas é dez e o encerramento máximo de contas é mil, mesmo que 10% das contas exceda mil. Para obter mais informações sobre as cotas do Organizations, consulte [Quotas for 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 assinaturas, primeiro [encerre todas as instâncias do 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 tiver sido suspenso e, dependendo do registrador do domínio, excluiríamos 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. Para obter mais 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 encerrar uma 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 da conta, consulte [Solução 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 encerrar uma conta autônoma na página Contas

1. [Faça login no Console de gerenciamento da AWS como usuário root](#) no Conta da AWS que você deseja fechar. Você não poderá encerrar uma conta se tiver feito login como usuário ou perfil do IAM.
2. No canto superior direito da barra de navegação, selecione o nome ou número da conta e, em seguida, selecione Conta.
3. Na página [Conta](#), escolha o botão Encerrar conta.
4. Digite o ID da 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 Encerrar conta para iniciar o processo de encerramento da conta.

6. Em alguns minutos, você receberá uma confirmação por e-mail de que a conta foi encerrada.

 Note


Essa tarefa não é suportada no AWS CLI ou por uma operação de API de um dos AWS SDKs. Você pode executar essa tarefa somente usando Console de gerenciamento da AWS 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 de 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. Essa opção só está disponível quando uma organização da AWS está no modo [Todos os atributos](#).

 Note

Se sua organização estiver usando o modo [Faturamento consolidado](#) o botão Encerrar não estará disponível no console. Para encerrar uma conta no modo de faturamento consolidado, entre na conta que você deseja encerrar como usuário-raiz. Na página Contas, clique o botão Encerrar conta, insira o ID da sua conta e clique o botão Encerrar conta.

4. Leia e certifique-se de que entendeu as orientações para o encerramento da conta.
5. Insira o ID da conta-membro e selecione Encerrar conta para iniciar o processo de encerramento da conta.

**Note**

Qualquer conta-membro que você encerrar exibirá uma etiqueta CLOSED ao lado do nome da conta no console do AWS Organizations por até 90 dias após a data de encerramento original. Depois de 90 dias, a conta-membro não será mais exibida no console do AWS Organizations .

Para encerrar uma conta-membro na página Contas

Opcionalmente, você pode fechar uma conta de AWS membro diretamente da [página Conta](#) no Console de gerenciamento da AWS. 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 e SDKs, 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 encerrar uma conta de gerenciamento diretamente no console do AWS Organizations .

Para encerrar uma conta de gerenciamento na página Contas

1. [Faça login Console de gerenciamento da AWS como usuário root da](#) conta de gerenciamento que você deseja fechar. Você não poderá encerrar uma conta se tiver feito login como usuário ou perfil do IAM.
2. Verifique se não há contas-membro ativas restantes em sua organização. Para fazer isso, acesse o [console do AWS Organizations](#) e verifique se todas as contas-membro estão mostrando Closed ao lado dos nomes das contas. Se você tiver uma conta-membro ainda

ativa, precisará seguir as orientações de encerramento de conta fornecidas na guia Conta-membro antes de passar para a próxima etapa.

3. No canto superior direito da barra de navegação, selecione o nome ou número da conta e, em seguida, selecione Conta.
4. Na página [Conta](#), escolha o botão Encerrar conta.
5. Digite o ID da 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 Encerrar conta para iniciar o processo de encerramento da conta.
7. Em alguns minutos, você receberá uma confirmação por e-mail de que a conta foi encerrada.

#### Note

Essa tarefa não é suportada no AWS CLI ou por uma operação de API de um dos AWS SDKs. Você pode executar essa tarefa somente usando Console de gerenciamento da AWS 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 encerrar a conta

Imediatamente após o encerramento da conta, ocorrerá o seguinte:

- Você receberá um e-mail confirmando o encerramento da conta no endereço de e-mail do usuário-raiz. Se você não receber esse e-mail em algumas horas, consulte [Solução de problemas com o Conta da AWS fechamento](#).

- Qualquer conta de membro que você fechar exibirá uma CLOSED etiqueta ao lado do nome da conta no AWS Organizations console por até 90 dias após a data de encerramento original. Após 90 dias, a conta do membro não será mais exibida no AWS Organizations console.
- Se você concedeu permissões para acessar serviços em suas Conta da AWS duas 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.

O encerramento da conta pode não ocorrer imediatamente em todas as regiões e serviços e pode levar várias horas para ser concluído.

## 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-encerramento é de 90 dias. Durante o período pós-encerramento, você só poderá acessar o conteúdo e os serviços da AWS se reabrir a conta. Após o período pós-fechamento, fecha AWS permanentemente o seu Conta da AWS e você não poderá mais reabri-lo. AWS também excluirá conteúdo e recursos da sua conta (exceto CloudTrail trilhas). Depois que uma conta tiver sido encerrada permanentemente, o [ID da Conta da AWS](#) 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 a conta antes que ela seja encerrada permanentemente, (1) você deverá entrar em contato com o [AWS Support](#) o quanto antes e (2) deveremos receber o pagamento integral de qualquer saldo pendente, incluindo o fornecimento das informações necessárias, conforme especificado na fatura, em até 60 dias a partir da data de encerramento da conta.

### Note

As cobranças pelos serviços que permaneceram na conta serão reiniciadas se você reabri-la.

# Referência da API

As operações de API no namespace Account Management (account) permitem que você modifique seu. Conta da AWS

Cada um Conta da AWS suporta 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 ao [usuário-raiz](#) da conta. Você pode especificar somente um de cada um dos tipos de contato a seguir associados a uma conta.

- Contato de faturamento
- Contato de operações
- Contato de segurança

Por padrão, as operações de API discutidas neste guia se aplicam diretamente à conta que chama a operação. A [identidade](#) da conta que está chamando a operação normalmente é um perfil 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 uma conta de AWS Organizations gerenciamento e especificar o número de ID da conta para qualquer pessoa Conta da AWS que seja 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 uma delas AWS SDKs, que consiste em bibliotecas e código de amostra para várias linguagens e plataformas de programação (Java, Ruby, .NET, iOS, Android e muito mais). Eles SDKs fornecem uma maneira conveniente de criar acesso programático às AWS Organizations. Por exemplo, SDKs cuidar da assinatura criptográfica de solicitações, do gerenciamento de erros e da repetição automática de solicitações. Para obter mais informações sobre o AWS SDKs, incluindo como baixá-los e instalá-los, consulte [Ferramentas para Amazon Web Services](#).

Recomendamos que você use o AWS SDKs para fazer chamadas programáticas de API para o serviço de gerenciamento de contas. No entanto, você também pode usar a API de consulta do Gerenciamento de Contas para fazer chamadas diretas para o serviço Web de Gerenciamento de Contas. Para saber mais sobre a API de consulta do Gerenciamento de Contas, consulte [Chamar a API por meio de solicitações de consulta HTTP](#) no Account Management User Guide. O Organizations oferece suporte a 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

Ao enviar solicitações HTTP para AWS, você deve assinar as solicitações para que AWS possa identificar quem as enviou. Você assina solicitações com sua chave de AWS acesso, que consiste em um ID de chave de acesso e uma chave de acesso secreta. É altamente recomendável não criar uma chave de acesso para o usuário-raiz. Qualquer pessoa que tenha a chave de acesso do usuário-raiz da conta tem acesso irrestrito a todos os recursos da conta. Em vez disso, crie uma chave de acesso para um usuário do IAM que tenha privilégios administrativos. Como outra opção, use o AWS Security Token Service para gerar credenciais de segurança temporárias e use essas credenciais para assinar solicitações.

Para assinar solicitações, recomendamos o uso do Signature Version 4. Se você tiver uma aplicação existente que usa o Signature Version 2, não precisará atualizá-la 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 [Solicitações de AWS API de assinatura](#) no Guia do usuário do IAM.

Quando você usa a Interface de Linha de AWS Comando (AWS CLI) ou uma das AWS SDKs para fazer solicitações AWS, essas ferramentas assinam automaticamente as solicitações para você com a chave de acesso que você especifica ao configurar as ferramentas.

### Suporte e feedback para o Gerenciamento de Contas

Os seus comentários são bem-vindos. Envie seu feedback para [feedback-awsaccounts@amazon.com](mailto:feedback-awsaccounts@amazon.com) ou publique seu feedback e suas perguntas no [Account Management support forum](#). Para obter mais informações sobre os fóruns de AWS suporte, consulte [a Ajuda dos fóruns](#).

### Como os exemplos são apresentados

O JSON retornado pelo Gerenciamento de Contas como resposta às suas solicitações é retornado como uma única string 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 leitura. Quando exemplos de parâmetros de entrada também resultam em sequências longas que se estendem para além da tela, inserimos quebras de linha para melhorar a leitura. Você deve sempre enviar a entrada como uma única string de texto JSON.

## Registro de solicitações de API

O Account Management suporta CloudTrail um serviço que registra chamadas de AWS API para você Conta da AWS e entrega arquivos de log em um bucket do Amazon S3. Usando as informações coletadas por CloudTrail, você pode determinar quais solicitações foram feitas com sucesso ao Gerenciamento de Contas, quem fez a solicitação, quando ela foi feita e assim por diante. Para obter mais informações sobre o gerenciamento de contas e seu suporte para CloudTrail, consulte [Registrando chamadas da API de gerenciamento de AWS contas usando AWS CloudTrail](#). Para saber mais sobre CloudTrail, inclusive como ativá-lo e encontrar seus arquivos de log, consulte o [Guia AWS CloudTrail do usuário](#).

## Ações

As ações a seguir são compatíveis:

- [AcceptPrimaryEmailUpdate](#)
- [DeleteAlternateContact](#)
- [DisableRegion](#)
- [EnableRegion](#)
- [GetAccountInformation](#)
- [GetAlternateContact](#)
- [GetContactInformation](#)
- [GetGovCloudAccountInformation](#)
- [GetPrimaryEmail](#)
- [GetRegionOptStatus](#)
- [ListRegions](#)
- [PutAccountName](#)
- [PutAlternateContact](#)

- [PutContactInformation](#)
- [StartPrimaryEmailUpdate](#)

## AcceptPrimaryEmailUpdate

Aceita a solicitação originada de [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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

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

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId.

Tipo: sequência

Padrão: `\d{12}`

Obrigatório: Sim

### Otp

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

Tipo: sequência

Padrão: `[a-zA-Z0-9]{6}`

Obrigatório: Sim

### PrimaryEmail

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

Tipo: string

Restrições de comprimento: tamanho mínimo de 5. O comprimento máximo é 64.

Obrigatório: 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 aceita de atualização do e-mail principal.

Tipo: string

Valores válidos: PENDING | ACCEPTED

## Erros

Para informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### ConflictException

Não foi possível processar a solicitação devido a um conflito no status atual do recurso. Por exemplo, isso acontece se você tenta habilitar uma região que está sendo desabilitada no momento (com status DESABILITANDO) ou se você tenta alterar o e-mail do usuário-raiz de uma conta para um endereço de e-mail que já está em uso.

errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de Status HTTP: 409

### InternalServerErrorException

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

errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### ResourceNotFoundException

Ocorreu uma falha na operação porque ela especificou um recurso que não pode ser encontrado.

errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 404

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

### ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

fieldList

O campo em que a entrada inválida foi detectada.

message

A mensagem que informa sobre o que era inválido na solicitação.

reason

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)

- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [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 [Update the alternate contacts for your Conta da AWS](#).

### 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 [Enable trusted access for AWS Account Management](#).

## 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 em uma conta de administrador delegado, e o ID da conta especificada deve ser de uma conta-membro na mesma organização. A organização deve ter [todos os atributos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

 Note

A conta de gerenciamento não pode especificar seu próprio AccountId; ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

Para chamar essa operação em uma conta que não seja 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: sequência

Padrão: `\d{12}`

Obrigatório: não

### [AlternateContactType](#)

Especifica quais contatos alternativos devem ser excluídos.

Tipo: string

Valores válidos: BILLING | OPERATIONS | SECURITY

Obrigatório: 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 informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerErrorException

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### ResourceNotFoundException

Ocorreu uma falha na operação porque ela especificou um recurso que não pode ser encontrado.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 404

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

## ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

`fieldList`

O campo em que a entrada inválida foi detectada.

`message`

A mensagem que informa sobre o que era inválido na solicitação.

`reason`

O motivo da falha na validação.

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

{
  "AccountName": "MyAccount"
}
```

### Resposta da amostra

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

### Exemplo 2

O exemplo a seguir exclui o contato alternativo para faturamento 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 uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

# DisableRegion

Desabilita (desativa) uma região específica para uma conta.

## Note

O ato de desabilitar 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 será 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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

**Note**

A conta de gerenciamento não pode especificar seu próprio AccountId. Ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

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: sequência

Padrão: `\d{12}`

Obrigatório: não

### RegionName

Especifica o código de 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 habilitar a região até que o processo de desabilitação esteja concluído.

Tipo: string

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

Obrigatório: 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 informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### ConflictException

Não foi possível processar a solicitação devido a um conflito no status atual do recurso. Por exemplo, isso acontece se você tenta habilitar uma região que está sendo desabilitada no momento (com status DESABILITANDO) ou se você tenta alterar o e-mail do usuário-raiz de uma conta para um endereço de e-mail que já está em uso.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de Status HTTP: 409

### InternalServerErrorException

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

## ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

fieldList

O campo em que a entrada inválida foi detectada.

message

A mensagem que informa sobre o que era inválido na solicitação.

reason

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

# EnableRegion

Habilita (ativa) 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 será 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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId. Ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

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: sequência

Padrão: `\d{12}`

Obrigatório: não

### RegionName

Especifica o código de 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 desabilitar a região até que o processo de habilitação esteja concluído.

Tipo: string

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

Obrigatório: 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 informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

### errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### ConflictException

Não foi possível processar a solicitação devido a um conflito no status atual do recurso. Por exemplo, isso acontece se você tenta habilitar uma região que está sendo desabilitada no momento (com status DESABILITANDO) ou se você tenta alterar o e-mail do usuário-raiz de uma conta para um endereço de e-mail que já está em uso.

### errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de Status HTTP: 409

### InternalServerErrorException

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

### errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

### errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

### ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

### fieldList

O campo em que a entrada inválida foi detectada.

## message

A mensagem que informa sobre o que era inválido na solicitação.

## reason

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

## GetAccountInformation

Recupera as informações sobre a conta especificada, incluindo nome e ID da conta e data e hora de criação da conta. Para usar essa API, um usuário do IAM ou perfil deve ter a permissão `account:GetAccountInformation` do IAM.

### Sintaxe da Solicitação

```
POST /getAccountInformation 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 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 em uma conta de administrador delegado, e o ID da conta especificada deve ser de uma conta-membro na mesma organização. A organização deve ter [todos os atributos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId; ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

Para chamar essa operação em uma conta que não seja 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: sequência

Padrão: `\d{12}`

Obrigatório: Não

## Sintaxe da resposta

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

{
  "AccountCreatedDate": "string",
  "AccountId": "string",
  "AccountName": "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.

### [AccountCreatedDate](#)


A data e a hora em que a conta foi criada.

Tipo: Timestamp

### [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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

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

 Note

A conta de gerenciamento não pode especificar seu próprio AccountId.

Tipo: sequência

Padrão: `\d{12}`

### AccountName

O nome da conta.

Tipo: string

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

Padrão: `[ - ; = ? - ~ ] +`

## Erros

Para informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerError

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

### ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

`fieldList`

O campo em que a entrada inválida foi detectada.

`message`

A mensagem que informa sobre o que era inválido na solicitação.

`reason`

O motivo da falha na validação.

Código de status HTTP: 400

## Exemplos

### Exemplo 1

O exemplo a seguir recupera as informações da conta para a conta cujas credenciais são usadas para chamar a operação.

### Exemplo de solicitação

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

{ }
```

## Resposta da amostra

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

{
  "AccountId": "123456789012",
  "AccountName": "MyAccount",
  "AccountCreateDate": "2020-11-30T17:44:37Z"
}
```

## Exemplo 2

O exemplo a seguir recupera as informações da conta para a conta de 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.GetAccountInformation

{
  "AccountId": "123456789012"
}
```

## Resposta da amostra

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

{
  "AccountId": "123456789012",
  "AccountName": "MyMemberAccount",
  "AccountCreateDate": "2020-11-30T17:44:37Z"
}
```

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [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 [Update the alternate contacts for your Conta da AWS](#).

### 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 [Enable trusted access for AWS Account Management](#).

## 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 em uma conta de administrador delegado, e o ID da conta especificada deve ser de uma conta-membro na mesma organização. A organização deve ter [todos os atributos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

 Note

A conta de gerenciamento não pode especificar seu próprio AccountId; ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

Para chamar essa operação em uma conta que não seja 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: sequência

Padrão: `\d{12}`

Obrigatório: não

### [AlternateContactType](#)

Especifica qual contato alternativo você deseja recuperar.

Tipo: string

Valores válidos: BILLING | OPERATIONS | SECURITY

Obrigatório: 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 informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerError

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### ResourceNotFoundException

Ocorreu uma falha na operação porque ela especificou um recurso que não pode ser encontrado.

### errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 404

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

### errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

### ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

### fieldList

O campo em que a entrada inválida foi detectada.

### message

A mensagem que informa sobre o que era inválido na solicitação.

### reason

O motivo da falha na validação.

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": "C00",
    "EmailAddress": "anika@example.com",
    "PhoneNumber": "206-555-0198",
    "AlternateContactType": "Security"
  }
}
```

## Exemplo 2

O exemplo a seguir recupera o contato alternativo das operações 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.GetAlternateContact

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

## Resposta da amostra

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

{
```

```
"AlternateContact":{
  "Name":"Anika",
  "Title":"C00",
  "EmailAddress":"anika@example.com",
  "PhoneNumber":"206-555-0198",
  "AlternateContactType":"Operations"
}
```

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

# GetContactInformation

Recupera as informações do contato principal de uma Conta da AWS.

Para obter detalhes completos sobre como usar as operações do contato principal, consulte [Update the primary contact for your Conta da AWS](#).

## 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 será 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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId. Ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

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: sequência

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 informações do contato principal associadas a uma Conta da AWS.

Tipo: objeto [ContactInformation](#)

## Erros

Para informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerErrorException

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### ResourceNotFoundException

Ocorreu uma falha na operação porque ela especificou um recurso que não pode ser encontrado.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 404

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

## ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

fieldList

O campo em que a entrada inválida foi detectada.

message

A mensagem que informa sobre o que era inválido na solicitação.

reason

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

## GetGovCloudAccountInformation

Recupera informações sobre a GovCloud conta vinculada à conta padrão especificada (se ela existir), incluindo o ID e o estado da GovCloud conta. Para usar essa API, um usuário do IAM ou perfil deve ter a permissão `account:GetGovCloudAccountInformation` do IAM.

### Sintaxe da Solicitação

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

{
  "StandardAccountId": "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.

#### StandardAccountId

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 em uma conta de administrador delegado, e o ID da conta especificada deve ser de uma conta-membro na mesma organização. A organização deve ter [todos os atributos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId; ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

Para chamar essa operação em uma conta que não seja 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: sequência

Padrão: `\d{12}`

Obrigatório: Não

## Sintaxe da resposta

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

{
  "AccountState": "string",
  "GovCloudAccountId": "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.

### AccountState

O estado da GovCloud conta vinculada.

Tipo: string

Valores válidos: PENDING\_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

### GovCloudAccountId

O número de identificação da conta de 12 dígitos da conta GovCloud vinculada.

Tipo: sequência

Padrão: `\d{12}`

## Erros

Para informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerError

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### ResourceNotFoundException

Ocorreu uma falha na operação porque ela especificou um recurso que não pode ser encontrado.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 404

### ResourceUnavailableException

A operação falhou porque especificou um recurso que não está disponível no momento.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 424

## TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

## ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

`fieldList`

O campo em que a entrada inválida foi detectada.

`message`

A mensagem que informa sobre o que era inválido na solicitação.

`reason`

O motivo da falha na validação.

Código de status HTTP: 400

## Exemplos

### Exemplo 1

O exemplo a seguir recupera as informações da GovCloud conta vinculada para a conta cujas credenciais são usadas para chamar a operação.

### Exemplo de solicitação

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetGovCloudAccountInformation
{}

```

### Resposta da amostra

```
HTTP/1.1 200 OK

```

```
Content-Type: application/json

{
  "GovCloudAccountId": "123456789012",
  "AccountState": "ACTIVE"
}
```

## Exemplo 2

O exemplo a seguir recupera as informações da GovCloud conta vinculada 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.GetGovCloudAccountInformation

{
  "StandardAccountId": "111111111111"
}
```

### Resposta da amostra

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

{
  "GovCloudAccountId": "123456789012",
  "AccountState": "ACTIVE"
}
```

## Exemplo 3

O exemplo a seguir tenta recuperar as informações da GovCloud conta vinculada para uma conta padrão que não está vinculada a uma GovCloud conta.

### Exemplo de solicitação

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

```
{  
  "StandardAccountId": "222222222222"  
}
```

## Resposta da amostra

```
HTTP/1.1 404  
Content-Type: application/json  
  
{  
  "message": "GovCloud Account ID not found for Standard Account - 222222222222."  
}
```

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

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

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId.

Tipo: sequência

Padrão: \d{12}

Obrigatório: 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: tamanho mínimo de 5. O comprimento máximo é 64.

## Erros

Para informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

errorType

O valor preenchido no cabeçalho da resposta x-amzn-ErrorType pelo API Gateway.

Código de status HTTP: 403

## InternalServerErrorException

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

## ResourceNotFoundException

Ocorreu uma falha na operação porque ela especificou um recurso que não pode ser encontrado.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 404

## TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

## ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

`fieldList`

O campo em que a entrada inválida foi detectada.

`message`

A mensagem que informa sobre o que era inválido na solicitação.

`reason`

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

# GetRegionOptStatus

Recupera o status de ativação 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 será 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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId. Ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

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: sequência

Padrão: `\d{12}`

Obrigatório: não

### RegionName

Especifica o código de 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.

Obrigatório: 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 (Habilitada, Sendo habilitada, Desabilitada, Sendo desabilitada, Habilitada\_por\_Padrão).

Tipo: string

Valores válidos: ENABLED | ENABLING | DISABLING | DISABLED |  
ENABLED\_BY\_DEFAULT

## Erros

Para informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerErrorException

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

errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

## ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

fieldList

O campo em que a entrada inválida foi detectada.

message

A mensagem que informa sobre o que era inválido na solicitação.

reason

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [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 ativação. Opcionalmente, essa lista pode ser filtrada pelo parâmetro `region-opt-status-contains`.

### 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 será 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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId. Ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

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: sequência

Padrão: `\d{12}`

Obrigatório: não

### MaxResults

O número total de itens para retornar na saída do comando. Se o número total de itens disponíveis for maior que o valor especificado, um `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: inteiro

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

Obrigatório: não

### NextToken

Um token para especificar onde iniciar a paginação. Esse é o `NextToken` de uma resposta truncada anteriormente. 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 (Sendo habilitada, Habilitada, Sendo desabilitada, Desabilitada, Habilitada\_por\_Padrão) a serem usados para filtrar a lista de regiões de uma determinada conta. Por exemplo, passar um valor `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. Deve ser passado para o parâmetro de solicitação `next-token` da `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 filtragem definidos no parâmetro `filter`.

Tipo: matriz de objetos [Region](#)

## Erros

Para informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerError

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

### ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

`fieldList`

O campo em que a entrada inválida foi detectada.

`message`

A mensagem que informa sobre o que era inválido na solicitação.

## reason

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

## PutAccountName

Atualiza o nome da conta especificada. Para usar essa API, a entidades principais do IAM devem ter a permissão `account:PutAccountName` do IAM.

### Sintaxe da Solicitação

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

{
  "AccountId": "string",
  "AccountName": "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 em uma conta de administrador delegado, e o ID da conta especificada deve ser de uma conta-membro na mesma organização. A organização deve ter [todos os atributos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

#### Note

A conta de gerenciamento não pode especificar seu próprio AccountId; ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

Para chamar essa operação em uma conta que não seja 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: sequência

Padrão: `\d{12}`

Obrigatório: não

### AccountName

O nome da conta.

Tipo: string

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

Padrão: `[ - ; = ? - ~ ] +`

Obrigatório: 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 informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerErrorException

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

### ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

`fieldList`

O campo em que a entrada inválida foi detectada.

`message`

A mensagem que informa sobre o que era inválido na solicitação.

`reason`

O motivo da falha na validação.

Código de status HTTP: 400

## Exemplos

### Exemplo 1

O exemplo a seguir atualiza o nome da conta cujas credenciais são usadas para chamar a operação.

## Exemplo de solicitação

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

{
  "AccountName": "MyAccount"
}
```

## Resposta da amostra

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

## Exemplo 2

O exemplo a seguir atualiza o nome da conta de 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.PutAccountName

{
  "AccountId": "123456789012",
  "AccountName": "MyMemberAccount"
}
```

## Resposta da amostra

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

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)

- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [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 [Update the alternate contacts for your Conta da AWS](#).

## 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 [Enable trusted access for AWS Account Management](#).

## 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 em uma conta de administrador delegado, e o ID da conta especificada deve ser de uma conta-membro na mesma organização. A organização deve ter [todos os atributos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

 Note

A conta de gerenciamento não pode especificar seu próprio AccountId; ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

Para chamar essa operação em uma conta que não seja 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: sequência

Padrão: `\d{12}`

Obrigatório: não

### [AlternateContactType](#)

Especifica qual contato alternativo você deseja criar ou atualizar.

Tipo: string

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]*`

Obrigatório: Sim

### Name

Especifica um nome para o contato alternativo.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. O comprimento máximo é 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()+- ]+`

Obrigatório: Sim

### Title

Especifica um título para o contato alternativo.

Tipo: string

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

Obrigatório: 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 informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerError

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

### ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

`fieldList`

O campo em que a entrada inválida foi detectada.

`message`

A mensagem que informa sobre o que era inválido na solicitação.

## reason

O motivo da falha na validação.

Código de status HTTP: 400

## Exemplos

### Exemplo 1

O exemplo a seguir define o contato alternativo para faturamento 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": "CF0",
  "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 para faturamento 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 uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

## PutContactInformation

Atualiza as informações do contato principal de uma Conta da AWS.

Para obter detalhes completos sobre como usar as operações do contato principal, consulte [Update the primary contact for your Conta da AWS](#).

### 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 será

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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os atributos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

 Note

A conta de gerenciamento não pode especificar seu próprio AccountId. Ela deve chamar a operação em um contexto autônomo sem incluir o parâmetro AccountId.

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: sequência

Padrão: `\d{12}`

Obrigatório: não

### [ContactInformation](#)

Contém os detalhes das informações do contato principal associadas a uma Conta da AWS.

Tipo: objeto [ContactInformation](#)

Obrigatório: 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 informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

### AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

### InternalServerError

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

### TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

### ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

`fieldList`

O campo em que a entrada inválida foi detectada.

`message`

A mensagem que informa sobre o que era inválido na solicitação.

## reason

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

# StartPrimaryEmailUpdate

Inicia o processo para atualizar o endereço de e-mail principal para a 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 em uma conta do administrador delegado. O ID da conta especificada deve ser uma conta-membro na mesma organização. A organização deve ter [todos os recursos habilitados](#) e deve ter [acesso confiável](#) habilitado para o serviço de gerenciamento de contas e, opcionalmente, uma conta do [administrador delegado](#) atribuída.

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

### Note

A conta de gerenciamento não pode especificar seu próprio AccountId.

Tipo: sequência

Padrão: \d{12}

Obrigatório: 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: tamanho mínimo de 5. O comprimento máximo é 64.

Obrigatório: 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 de atualização do e-mail principal.

Tipo: string

Valores válidos: PENDING | ACCEPTED

## Erros

Para informações sobre os erros comuns retornados pelas ações, consulte [Erros comuns](#).

## AccessDeniedException

Ocorreu uma falha na operação porque a identidade de chamada não tem as permissões mínimas necessárias.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 403

## ConflictException

Não foi possível processar a solicitação devido a um conflito no status atual do recurso. Por exemplo, isso acontece se você tenta habilitar uma região que está sendo desabilitada no momento (com status DESABILITANDO) ou se você tenta alterar o e-mail do usuário-raiz de uma conta para um endereço de e-mail que já está em uso.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de Status HTTP: 409

## InternalServerErrorException

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

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 500

## ResourceNotFoundException

Ocorreu uma falha na operação porque ela especificou um recurso que não pode ser encontrado.

`errorType`

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 404

## TooManyRequestsException

Ocorreu uma falha na operação porque ela foi chamada com muita frequência e excedeu um limite de controle de utilização.

## errorType

O valor preenchido no cabeçalho da resposta `x-amzn-ErrorType` pelo API Gateway.

Código de status HTTP: 429

## ValidationException

Ocorreu uma falha na operação porque um dos parâmetros de entrada era inválido.

### fieldList

O campo em que a entrada inválida foi detectada.

### message

A mensagem que informa sobre o que era inválido na solicitação.

### reason

O motivo da falha na validação.

Código de Status HTTP: 400

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Interface de linha de comando V2](#)
- [AWS SDK para .NET V4](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

## Ações relacionadas em outros AWS serviços

As operações a seguir estão relacionadas AWS Gerenciamento de contas , mas fazem parte do AWS Organizations namespace:

- [CreateAccount](#)
- [CreateGovCloudAccount](#)
- [DescribeAccount](#)

### CreateAccount

A operação da `CreateAccount` API está disponível para uso somente no contexto de uma organização gerenciada pelo AWS Organizations serviço. A operação da API é definida no namespace desse serviço.

Para obter mais informações, consulte [CreateAccount](#) na Referência de APIs do AWS Organizations

### CreateGovCloudAccount

A operação da `CreateGovCloudAccount` API está disponível para uso somente no contexto de uma organização gerenciada pelo AWS Organizations serviço. A operação da API é definida no namespace desse serviço.

Para obter mais informações, consulte [CreateGovCloudAccount](#) na Referência de APIs do AWS Organizations .

### DescribeAccount

A operação da `DescribeAccount` API está disponível para uso somente no contexto de uma organização gerenciada pelo AWS Organizations serviço. A operação da API é definida no namespace desse serviço.

Para obter mais informações, consulte [DescribeAccount](#) na Referência de APIs do AWS Organizations .

## 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 conta da AWS

## Conteúdo

### AlternateContactType

O tipo de contato alternativo.

Tipo: string

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. O comprimento máximo é 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 uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

## ContactInformation

Contém os detalhes das informações do contato principal associadas a uma Conta da AWS.

### Conteúdo

#### AddressLine1

A primeira linha do endereço do contato principal.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. O comprimento máximo é 60.

Obrigatório: Sim

#### City

A cidade do endereço do contato principal.

Tipo: string

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

Obrigatório: Sim

#### CountryCode

O código ISO-3166 de duas letras do país do endereço do contato principal.

Tipo: string

Restrições de comprimento: comprimento fixo de 2.

Obrigatório: Sim

#### FullName

O nome completo do endereço do contato principal.

Tipo: string

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

Obrigatório: Sim

## PhoneNumber

O número de telefone das informações do contato principal. O número será validado e, em alguns países, verificado para ativação.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 20.

Padrão: `[+][\s0-9()-]+`

Obrigatório: Sim

## PostalCode

O código postal do endereço do contato principal.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Tamanho máximo de 20.

Obrigatório: Sim

## AddressLine2

A segunda linha do endereço do contato principal, se houver.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 60.

Obrigatório: não

## AddressLine3

A terceira linha do endereço do contato principal, se houver.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 60.

Obrigatório: não

## CompanyName

O nome da empresa associada às informações do contato principal, se houver.

Tipo: string

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

Obrigatório: não

#### DistrictOrCounty

O distrito ou condado do endereço do contato principal, se houver.

Tipo: string

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

Obrigatório: não

#### StateOrRegion

O estado ou a região do endereço do contato principal. Se o endereço de correspondência estiver nos Estados Unidos (EUA), o valor nesse campo poderá 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: US, CA, GB, DE, JP, IN e BR.

Tipo: string

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

Obrigatório: não

#### WebsiteUrl

O URL do site associado às informações do contato principal, se houver.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. O comprimento máximo é 256.

Obrigatório: Não

## Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para 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 no status de ativação.

### Conteúdo

#### RegionName

O código de uma determinada região (por exemplo, `us-east-1`).

Tipo: string

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

Obrigatório: não

#### RegionOptStatus

Um dos possíveis status que uma região pode ter (Habilitada, Sendo habilitada, Desabilitada, Sendo desabilitada, Habilitada\_por\_Padrão).

Tipo: string

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

Obrigatório: não

### Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para 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 uma das linguagens específicas AWS SDKs, 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 de AWS 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 YYYY-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\_aceso/AAAAMMDD/região/serviço/aws4\_request.

Para obter mais informações, consulte [Criar uma solicitação de AWS 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 e hora a seguir é um X-Amz-Date valor válido:20120325T120000Z.

Condição: X-Amz-Date é opcional para todas as solicitações; ele pode ser usado para substituir a data usada em solicitações de assinatura. Se o cabeçalho da data for especificado no formato básico ISO 8601, não X-Amz-Date é necessário. Quando X-Amz-Date usado, ele sempre substitui o valor do cabeçalho da data. Para obter mais informações, consulte [Elementos de uma assinatura de solicitação de AWS API](#) no Guia do usuário do IAM.

Tipo: string

Obrigatório: Condicional

### X-Amz-Security-Token

O token de segurança temporário obtido por meio de uma chamada para AWS Security Token Service (AWS STS). Para obter uma lista de serviços que oferecem suporte a credenciais de segurança temporárias do AWS STS, consulte [Serviços da AWS que funcionam com o IAM](#) no Guia do usuário do IAM.

Condição: se você estiver usando credenciais de segurança temporárias do AWS STS, 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 a especificação de cabeçalhos assinados, consulte [Criar uma solicitação de AWS 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 AWS serviços. 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 está em conformidade com os AWS padrões.

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 ID da chave de AWS acesso 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 AWS acesso precisa de uma assinatura para o serviço.

Código de status HTTP: 403

#### RequestExpired

A solicitação chegou ao serviço mais de 15 minutos após o carimbo de data na solicitação ou mais de 15 minutos após a data de expiração da solicitação (como para pré-assinada URLs), ou o carimbo de data na solicitação é 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 satisfaz as restrições especificadas por um AWS serviço.

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 para gerenciamento de AWS 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 a API de consulta de gerenciamento de AWS contas, você pode usar um dos AWS SDKs. Eles AWS SDKs consistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação (Java, Ruby, .NET, iOS, Android e muito mais). Eles SDKs fornecem uma maneira conveniente de criar acesso programático ao gerenciamento de AWS contas e. AWS Por exemplo, SDKs cuidar de tarefas como assinar criptograficamente solicitações, gerenciar erros e repetir solicitações automaticamente. Para obter informações sobre o AWS SDKs, incluindo como baixá-los e instalá-los, consulte [Ferramentas para Amazon Web Services](#).

Com a API de consulta para gerenciamento de AWS 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 Suporte GET e POST solicitações de gerenciamento de contas para todas as operações. 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 de tamanho de um URL. Embora esse limite dependa do navegador, um limite típico é 2.048 bytes. Portanto, para as solicitações da API de consulta que exigem tamanhos maiores, você deve usar uma solicitação POST.

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](#)
- [Assinar solicitações da API de gerenciamento de AWS contas](#)

## Endpoints

AWS O 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 AWS endpoints e regiões para todos os serviços, consulte [Regiões e endpoints](#) no. Referência geral da AWS

## HTTPS obrigatório

Como a API de consulta pode retornar informações confidenciais, como credenciais de segurança, você deve usar HTTPS para criptografar todas as solicitações de API.

## Assinar solicitações da API de gerenciamento de AWS 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 as credenciais da sua conta AWS raiz para o trabalho diário com o Gerenciamento de AWS Contas. Você pode usar as credenciais de um usuário AWS Identity and Access Management (IAM) ou credenciais temporárias, como as usadas com uma função do IAM.

Para assinar suas solicitações de API, você deve usar o AWS Signature versão 4. Para obter informações sobre como usar o Signature versão 4, consulte [Solicitações de AWS API de assinatura](#) no Guia do usuário do IAM.

Para saber mais, consulte:

- [Credenciais de segurança da AWS](#): fornece informações gerais sobre os tipos de credencial que você pode usar para acessar a AWS.
- [Práticas recomendadas de segurança no IAM](#) — Oferece sugestões para usar o serviço IAM para ajudar a proteger seus AWS recursos, incluindo aqueles no gerenciamento de AWS contas.
- [Credenciais de segurança temporárias no IAM](#): descreve como criar e usar credenciais de segurança temporárias.

## Cotas para AWS Gerenciamento de contas

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 solicitações StartPrimaryEmailUpdate por conta de destino	Três por 30 segundos
Número de contatos alternativos em um Conta da AWS	Três: cada um para BILLING, SECURITY e OPERATIONS
Número de solicitações simultâneas de opções de ativação ou desativação de uma região por conta	6
Número de solicitações simultâneas de opções de ativação ou desativação de uma região por organização	50
Taxa de solicitações AcceptPrimaryEmailUpdate por conta de chamador	Uma por segundo, intermitência de até uma por segundo
Taxa de solicitações DeleteAlternateContact por conta	Uma por segundo, intermitência de até seis por segundo
Taxa de solicitações DisableRegion por conta	Uma por segundo, intermitência de até uma por segundo
Taxa de solicitações EnableRegion por conta	Uma por segundo, intermitência de até uma por segundo
Taxa de solicitações GetAccountInformation por conta de chamador	Três por segundo, intermitência de até três por segundo

Recurso	Quota
Taxa de solicitações <code>GetAlternateContact</code> por conta	10 por segundo, intermitência de até 15 por segundo
Taxa de solicitações <code>GetContactInformation</code> por conta	10 por segundo, intermitência de até 15 por segundo
Taxa de solicitações <code>GetGovCloudAccountInformation</code> por conta	Três por segundo, intermitência de até cinco por segundo
Taxa de solicitações <code>GetPrimaryEmail</code> por conta de chamador	Três por segundo, intermitência de até três por segundo
Taxa de solicitações <code>GetRegionOptStatus</code> por conta	Cinco por segundo, intermitência de até cinco por segundo
Taxa de solicitações <code>ListRegions</code> por conta	Cinco por segundo, intermitência de até cinco por segundo
Taxa de solicitações <code>PutAccountName</code> por conta de chamador	Uma por segundo, intermitência de até uma por segundo
Taxa de solicitações <code>PutAlternateContact</code> por conta	Cinco por segundo, intermitência de até oito por segundo
Taxa de solicitações <code>PutContactInformation</code> por conta	Cinco por segundo, intermitência de até oito por segundo
Taxa de solicitações <code>StartPrimaryEmailUpdate</code> por conta de chamador	Uma por segundo, intermitência de até uma por segundo

# Gerenciar contas na Índia

Se você se inscrever em um novo Conta da AWS e escolher a Índia como seu endereço de contato e cobrança, seu contrato de usuário será com a Amazon Web Services India Private Limited (AWS Índia), um AWS vendedor local na Índia. AWS A Índia gerencia seu faturamento e o total da fatura é listado em rúpias indianas (INR) em vez de dólares americanos (USD). Para obter informações sobre como gerenciar um Conta da AWS, consulte [Configure seu Conta da AWS](#).

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

Como parte da verificação do cartão de crédito durante a inscrição, a AWS Índia cobra 2 INR do seu cartão de crédito. AWS A Índia reembolsa os 2 INR após a verificação ser feita. Você pode ser redirecionado para seu banco como parte do processo de verificação.

## Tópicos

- [Crie um Conta da AWS com a AWS Índia](#)
- [Gerenciar suas informações de verificação do cliente](#)

## Crie um Conta da AWS com a AWS Índia

AWS A Índia é um vendedor local AWS de na Índia. Se seu endereço de contato e cobrança estiver na Índia e você quiser criar uma conta, use o procedimento a seguir para se inscrever em uma conta na AWS Índia.

Para se inscrever em uma conta AWS na Índia

1. Abra a [página inicial da Amazon Web Services](#).
2. Escolha Criar um Conta da AWS.

### Note


Se você se conectou AWS recentemente, essa opção pode não estar lá. Em vez disso, escolha Fazer login no console. Se a opção Criar uma nova Conta da AWS ainda não

estiver exibida, escolha Fazer login em uma conta diferente e, em seguida, escolha Criar uma nova Conta da AWS.

3. Insira as informações da conta, verifique o endereço de e-mail e escolha uma senha forte para a conta.
4. Escolha Comercial ou Pessoal. Contas pessoais e comerciais têm os mesmos recursos e funções.
5. Insira suas informações de contato pessoais ou da empresa. Se seu endereço de contato ou cobrança estiver na Índia, em conformidade com os regulamentos da Equipe Indiana de Resposta a Emergências de Computadores (CERT-In), AWS é necessário coletar e validar suas informações de identidade antes de conceder acesso aos serviços. AWS

O nome que você escolher para informações de contato ou faturamento deverá corresponder ao nome que consta do documento que você planeja usar para verificação do cliente. Por exemplo, se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento. Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).

6. Depois de ler o contrato de cliente, marque a caixa de seleção referente aos termos e condições e escolha Continuar.
7. Na página Billing information (Informações de faturamento), insira o método de pagamento que deseja usar. É necessário fornecer o CVV como parte do processo de verificação.
8. Em Você tem um PAN?, escolha Sim se você tiver um número de conta permanente (PAN) que gostaria que fosse exibido nas notas fiscais e, em seguida, insira o PAN. Se você não tiver um PAN ou se quiser adicioná-lo após o cadastro, escolha Não.
9. Escolha Verificar e continuar. AWS A Índia cobra 2 INR do seu cartão como parte do processo de verificação. AWS A Índia reembolsa os 2 INR após a verificação ser feita.
10. Na página Confirmar sua identidade, selecione o objetivo principal do registro da conta.
11. Escolha o tipo de propriedade que representa melhor o proprietário da conta. Se você escolher uma empresa, organização ou parceria como tipo de propriedade, insira o nome de um dos principais membros da administração. Essa pessoa pode ser um diretor, um chefe de operações ou uma pessoa responsável pelas operações da empresa.
12. Dependendo do tipo de propriedade selecionado, escolha um tipo de documento aceito na Índia para usar na verificação e insira as informações do documento.

 Note

Se você tem uma conta pessoal e planeja usar uma carteira de habilitação que não seja emitida pela União da Índia, é recomendável usar um tipo de documento pessoal diferente para verificação.


13. Escolha o nome que você deseja usar para verificação do cliente.

Os nomes das suas informações de faturamento e contato serão exibidos para seleção se estiverem associados a um endereço indiano. Certifique-se de que o nome que você escolher corresponda ao nome que consta do tipo de documento que você planeja usar para a verificação do cliente. Se você precisar fazer alterações no nome associado ao endereço de faturamento ou contato, poderá fazer isso depois de concluir o cadastramento na conta.

14. Forneça seu consentimento para enviar as informações para verificação e escolha Continuar.

Você receberá uma notificação sobre o resultado da verificação do cliente por e-mail depois de concluir o cadastro na conta. Você também pode verificar o status na página de verificação do cliente nas configurações da sua conta ou no AWS Health Dashboard posteriormente. Você deve passar na verificação do cliente para acessar os serviços da AWS .

15. Escolha se deseja verificar o número do seu celular por Mensagem de texto (SMS) ou Chamada de voz.
16. Escolha seu país ou código de região e, em seguida, insira seu número de celular.
17. Complete a verificação de segurança.
18. Escolha Enviar SMS ou Ligar para mim agora. Depois de alguns momentos, você receberá um pin de quatro dígitos em um SMS ou em uma chamada automatizada no celular.
19. Na página Confirmar sua identidade, insira o pin que você recebeu e escolha Continuar.
20. Na página Selecione um plano de suporte, selecione o plano de suporte e, em seguida, escolha Concluir cadastramento. Depois que o método de pagamento for verificado e a verificação do cliente for concluída, a conta será ativada e você receberá um e-mail confirmando a ativação da conta.

 Note

Se você tiver concluído a verificação do cliente e tiver editado o nome, o endereço ou o tipo de documento anteriormente usado para verificar sua identidade, talvez seja

necessário passar pela verificação do cliente novamente. Para obter mais informações, consulte [the section called “Editar suas informações de verificação do cliente”](#).

## Gerenciar suas informações de verificação do cliente

Em conformidade com os regulamentos da Equipe Indiana de Resposta a Emergências de Computadores (CERT-In), AWS é necessário coletar e validar suas informações de identidade antes de conceder a você acesso novo ou contínuo aos serviços. AWS Sua identidade deve ser verificada usando o nome fornecido por você no endereço de faturamento ou de contato na Índia. Durante a verificação, AWS verificará se o número do documento é válido e se o nome fornecido corresponde ao nome associado ao documento usado para verificação do cliente. O nome que você escolher para informações de contato ou faturamento deverá corresponder exatamente ao nome que consta do documento.

Para atualizar seu nome e endereço de faturamento, consulte a página [Preferências de pagamento](#). Para atualizar seu nome e endereço de contato, consulte [the section called “Atualize o contato principal do seu Conta da AWS”](#). Se você editar as informações que usou anteriormente para a verificação do cliente, como o nome ou o endereço na Índia das suas informações de faturamento ou contato, talvez precise atualizar e reenviar suas informações de verificação do cliente.

## Verificar o status da sua verificação do cliente

Você pode verificar o status da sua verificação do cliente a qualquer momento na página Verificação do cliente. Se o status da sua verificação for Verificação necessária ou Falha na verificação, crie ou atualize suas informações de verificação do cliente e envie-as novamente para verificação.

## Criar suas informações de verificação do cliente

Para concluir a verificação do cliente, você precisará fornecer informações de um documento aceito na Índia. Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).

1. Faça login no [Console de gerenciamento da AWS](#).
2. No canto superior direito da barra de navegação, escolha o nome (ou alias) da conta e escolha Conta.
3. Em Other settings (Outras configurações), escolha Customer verification (Verificação do cliente).

Se você ainda não tiver fornecido as informações de verificação do cliente, a página Criar verificação do cliente será exibida.

- Escolha um nome que corresponda exatamente ao nome que consta do documento que você planeja usar para a verificação do cliente. Por exemplo, se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento.
- Forneça as informações remanescentes solicitadas na página. Dependendo do tipo de documento escolhido, talvez seja necessário carregar uma cópia da frente e do verso do documento. Se você carregar um arquivo de imagem, verifique se todas as informações constantes do documento estão visíveis e legíveis.
- Selecione Enviar.

Você será notificado sobre o resultado da verificação do cliente e sobre as próximas etapas por e-mail ou no AWS Health Dashboard.

## Editar suas informações de verificação do cliente

Você pode editar suas informações de verificação do cliente, como o objetivo principal do registro da conta, o tipo de organização e o nome, o tipo de documento, o carregamento do documento ou as informações do documento que você deseja usar para verificação.

Se você editar o nome ou o tipo de documento a ser usado na verificação do cliente ou se atualizar quaisquer informações do documento, para salvar as alterações será necessário verificar sua identidade novamente.

- Faça login no [Console de gerenciamento da AWS](#).
- No canto superior direito da barra de navegação, escolha o nome (ou alias) da conta e escolha Conta.
- Em Other settings (Outras configurações), escolha Customer verification (Verificação do cliente).
- Escolha Editar e, em seguida, atualize as informações que você deseja alterar.

Ao atualizar as informações, observe as seguintes orientações:

- Se você escolher um nome diferente, o nome deverá corresponder exatamente ao nome que consta do documento que você planeja usar para a verificação do cliente. Por exemplo, se

Se você planeja verificar uma conta comercial usando um Certificado de Incorporação social, deve fornecer o nome comercial que consta do documento.

- Se você escolher um tipo de documento diferente, precisará carregar uma cópia da frente e do verso (se aplicável) do documento. Todas as informações no carregamento do documento devem estar visíveis e legíveis.
- Se você tem uma conta pessoal e planeja usar uma carteira de habilitação que não seja emitida pela União da Índia, é recomendável usar um tipo de documento pessoal diferente para verificação.

Para obter uma lista dos tipos de documentos aceitos, consulte [the section called “Documentos da Índia aceitos para verificação do cliente”](#).

## 5. Selecione Enviar.

Se sua identidade precisar ser verificada novamente devido ao tipo de alteração que você salvou, você receberá uma notificação do resultado da verificação do cliente e das próximas etapas por e-mail. Você também pode ver os resultados retornando à página de verificação do cliente ou ao AWS Health Dashboard.

## Documentos da Índia aceitos para verificação do cliente

Os seguintes tipos de documentos emitidos pelo governo indiano são aceitos para verificação do cliente.

### Note

Os links compartilhados abaixo estão sujeitos a alterações pelo governo.

- **Cartão de PAN:** disponível em formato digital e físico, o cartão de número de conta permanente (PAN) contém um identificador alfanumérico exclusivo emitido pelo Income Tax Department of India para indivíduos, empresas e entidades. Um PAN consiste em dez caracteres, incluindo letras e números, no formato **AAAAA1111A**. Para usar esse documento para verificação, você também deve fornecer a data de nascimento (pessoa física) ou a data de incorporação (empresa) exibida no cartão de PAN e carregar a frente do cartão. Consulte o [site oficial do Income Tax Department](#) para verificar a validade do PAN.
- **Título de eleitor/EPIC:** o título de eleitor, também conhecido como Cartão de Identidade com Foto do Eleitor (EPIC), contém um número de identificação exclusivo emitido pela Election

Commission of India para eleitores qualificados na Índia. O ID/EPIC número do eleitor consiste em dez caracteres, incluindo letras e números. Acesse o site oficial da [Election Commission of India](#) para verificar a validade do seu título de eleitor. Para usar esse documento para verificação, você deve carregar a frente e o verso do cartão.

- Carteira de habilitação: se sua carteira de habilitação não for emitida pela União da Índia, recomendamos o uso de um tipo de documento diferente para verificação. O número da carteira de habilitação consiste em 12 a 16 caracteres, incluindo letras, números e um espaço ou hífen. Para usar esse documento para verificação, você deve informar sua data de nascimento e carregar a frente e o verso do cartão. Acesse o [site Parivahan Sewa](#) do Ministry of Road Transport and Highways para verificar a validade da sua carteira de habilitação.
- Certificado de Incorporação: um certificado de incorporação é um documento emitido pelo Ministry of Corporate Affairs (MCA), que data o registro de uma empresa como pessoa jurídica. O certificado é usado para identificar e rastrear de forma exclusiva empresas registradas na Índia. Cada certificado contém um Número de Identificação Corporativa (CIN), que é um identificador alfanumérico exclusivo que consiste em 21 caracteres, incluindo letras e números. Para usar esse documento para verificação, você deve carregar o documento do certificado de incorporação. Você pode acessar o [portal do Ministry of Corporate Affairs](#) para verificar a validade do CIN.

Diferentes tipos de documentos da Índia são aceitos para contas pessoais e comerciais:

- Para contas pessoais: cartão PAN, título de eleitor/EPIC e carteira de habilitação.
- Para contas comerciais: cartão de PAN e certificado de incorporação.

## Gerencie sua AWS conta na Índia

Com exceção das tarefas a seguir, os procedimentos para o gerenciamento da conta são os mesmos das contas criadas fora da Índia. Para obter informações gerais sobre como gerenciar a conta, consulte [Configurar a conta](#).

Use o Console de gerenciamento da AWS para realizar as seguintes tarefas:

- [Adicionar ou editar um número de conta permanente](#)
- [Editar vários números de conta permanente](#)
- [the section called “Gerenciar suas informações de verificação do cliente”](#)
- [Editar vários números fiscais de bens e serviços \(GSTs\)](#)
- [Visualizar uma fatura fiscal](#)

# Histórico do documento para o Account Management User Guide

A tabela a seguir descreve os lançamentos da documentação para gerenciamento de AWS contas.

Alteração	Descrição	Data
<a href="#">Novo nome da conta APIs</a>	Support para novos <a href="#">GetAccountInformation</a> nomes e <a href="#">PutAccountName</a> APIs para visualizar ou modificar um nome de conta.	22 de abril de 2025
<a href="#">Fim do suporte para edição das perguntas de desafio de segurança</a>	O tópico Editar suas perguntas de desafio de segurança foi removido do guia após o término do suporte.	6 de janeiro de 2025
<a href="#">Novo e-mail principal APIs</a>	Support para novos <a href="#">GetPrimaryEmail</a> , <a href="#">StartPrimaryEmailUpdate</a> , e <a href="#">AcceptPrimaryEmailUpdate</a> APIs para atualizar centralmente o endereço de e-mail do usuário raiz, endereço de , para qualquer conta membro em AWS Organizations. Para obter mais informações, consulte <a href="#">Updating the root user email address para uma conta de membro</a> no Guia do usuário do AWS Organizations .	6 de junho de 2024

<a href="#">Reescrita do tópico de encerramento de contas</a>	Retificação completa de todo o tópico de encerramento de contas, incluindo a adição de etapas sobre como fechar contas-membro e de gerenciamento.	1.º de fevereiro de 2024
<a href="#">Fim do suporte para a adição de novas perguntas de desafio de segurança</a>	Adicionado novo conteúdo observando que a opção de adicionar novas perguntas de desafio foi removida da página Contas.	5 de janeiro de 2024
<a href="#">Fim do suporte para o namespace aws-portal</a>	AWS Identity and Access Management As ações (IAM) que eram usadas anteriormente para gerenciar sua conta (por exemplo, <code>aws-portal:ModifyAccount</code> e <code>aws-portal:ViewAccount</code> ) chegaram ao fim do suporte padrão.	1º de janeiro de 2024
<a href="#">Reescrita do tópico Regiões</a>	Retificado por completo todo o tópico Regiões, incluindo a adição de controles para expandir e recolher.	8 de outubro de 2023
<a href="#">Realocados tópicos do usuário-raiz para o Guia do usuário do IAM</a>	Consolidada a discussão sobre usuários-raiz em um tópico, adicionados links de referência cruzada aos tópicos do usuário-raiz que foram movidos para o Guia do usuário do IAM.	18 de setembro de 2023

---

<a href="#">Nova seção adicionada ao tópico de contato da conta principal</a>	Adicionada uma nova seção Requisitos de número de telefone e endereço de e-mail.	12 de setembro de 2023
<a href="#">Novas informações de contato APIs</a>	Support for new GetContactInformation PutContactInformation APIs e.	22 de julho de 2022
<a href="#">AWS O gerenciamento de contas agora suporta a atualização de contatos alternativos por meio do AWS Organizations console.</a>	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
<a href="#">Lançamento inicial</a>	Versão inicial do Guia de referência de gerenciamento de AWS contas	30 de setembro de 2021

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.