Manual do usuário

# AWS Organizations

# AWS Organizations: Manual do usuário

# Table of Contents

# O que é o AWS Organizations?

O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias contas da Contas da AWS em uma única organização que você cria e gerencia centralmente. O AWS Organizations inclui todas as funcionalidades de gerenciamento de contas e de faturamento consolidado que permitem atender melhor às necessidades de orçamento, segurança e compatibilidade de sua empresa. Como um administrador de uma organização, você pode criar contas em sua organização e convidar contas existentes a participarem da organização.

Este guia do usuário define os -principais conceitos do AWS Organizations, fornece tutoriais, e explica como criar e gerenciar uma organização.

Tópicos



## Recursos do AWS Organizations

A AWS Organizations oferece os seguintes recursos:

Gerenciamento centralizado de todas as suas Contas da AWS

> 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.

Faturamento consolidado para todas as contas de membros

> Faturamento consolidado é um recurso do AWS Organizations. Você pode usar a conta de gerenciamento de sua organização para consolidar e pagar para todas as contas-membro. No faturamento consolidado, as contas de gerenciamento também podem acessar as informações de faturamento, informações de conta e atividade das contas-membro de sua organização. Essas informações podem ser usadas em serviços, como o Cost Explorer, que podem ajudar as contas de gerenciamento a melhorar a performance em custos de sua organização.

Agrupamento hierárquico de suas contas para atender às necessidades de orçamento, segurança ou conformidade

Você pode agrupar suas contas em organizational units (UOs – unidades organizacionais) e anexar diferentes políticas de acesso para cada UO. Por exemplo, se você tiver contas que devam acessar apenas os serviços da AWS que atendem a certos requisitos normativos, pode colocar as contas em uma UO. Em seguida, pode anexar uma política para essa UO que bloqueie o acesso a serviços que não atendam a esses requisitos normativos. Você pode aninhar UOs com outras UOs, chegando até a cinco níveis, fornecendo flexibilidade para estruturar seus grupos de contas.

Políticas para centralizar o controle sobre os serviços da AWS e as ações da API que cada conta pode acessar

Como administrador da conta de gerenciamento de uma organização, você pode usar políticas de controle de serviço (SCPs - service control policies) para especificar o máximo de permissões para as contas-membro da organização. Nas SCPs, você pode restringir os serviços, recursos e ações individuais de API da AWS que os usuários e funções em cada conta-membro podem acessar. Você também pode definir condições para quando o acesso aos serviços, recursos e ações de API da AWS deve ser restringido. Essas restrições substituem até mesmo os administradores de contas-membro da organização. Quando o AWS Organizations bloqueia o acesso a um serviço, recurso ou ação de API para uma conta-membro, um usuário ou função nessa conta não pode acessá-lo. Esse bloqueio permanece em vigor mesmo que um administrador de uma conta-membro conceda explicitamente essas permissões em uma política do IAM.

Para mais informações, consulte Políticas de controle de serviço (SCPs).

Políticas para padronizar tags em todos os recursos das contas da organização

Você pode usar políticas de tag para manter tags consistentes, incluindo o tratamento preferencial de maiúsculas e minúsculas de chaves e valores de tag.

Para obter mais informações, consulte Políticas de tag.

Políticas para controlar como os serviços de inteligência artificial (IA) e machine learning da AWS podem coletar e armazenar dados.

Você pode usar políticas de exclusão de serviços de IA para excluir a coleta e o armazenamento de dados para qualquer um dos serviços de IA da AWS que você não deseje usar.

Para obter mais informações, consulte Políticas de exclusão dos serviços de IA.

Políticas que configuram backups automáticos para os recursos das contas da organização

Você pode usar políticas de backup para configurar e aplicar automaticamente planos de AWS Backup para os recursos de todas as contas de sua organização.

Para obter mais informações, consulte Políticas de backup.

Integração e suporte para o AWS Identity and Access Management (IAM)

O IAM fornece controle detalhado sobre os usuários e as funções em contas individuais. O AWS Organizations expande esse controle para o nível de conta, dando a você controle sobre o que os usuários e as funções de uma conta ou grupo de contas podem fazer. As permissões resultantes são a interseção lógica do que é permitido pelo AWS Organizations no nível da conta e as permissões que são explicitamente concedidas pelo IAM no nível de usuário ou de função dentro dessa conta. Em outras palavras, o usuário pode acessar apenas o que é permitido por ambos, as políticas do AWS Organizations e pelas políticas do IAM. Se uma delas bloquear uma operação, o usuário não poderá acessá-la.

Integração com outros serviços da AWS

É possível utilizar os serviços de gerenciamento de várias contas disponíveis no AWS Organizations com serviços selecionados da AWS para executar tarefas em todas as contas que são membros da uma organização. Para obter uma lista dos serviços e os benefícios de usar cada serviço em nível de toda a organização, consulte AWS serviços que você pode usar com AWS Organizations.

Quando você habilita um serviço da AWS para executar tarefas em seu nome nas contas-membro da organização, o AWS Organizations cria uma função vinculada ao serviço do IAM para esse serviço em cada conta-membro. A função vinculada ao serviço tem permissões predefinidas do IAM que possibilitam que outro serviço da AWS execute tarefas específicas em sua organização e em suas contas. Para que isso funcione, todas as contas em uma organização têm automaticamente uma função vinculada ao serviço. Essa função permite que o serviço do AWS Organizations crie as funções vinculadas ao serviço exigidas pelos serviços da AWS para os quais você habilita o acesso confiável. Essas funções vinculadas ao serviço adicionais são associadas a políticas do IAM que permitem que o serviço especificado execute apenas as tarefas que são exigidas por suas opções de configuração. Para mais informações, consulte Usar o AWS Organizations com outros serviços da AWS.

Acesso global

O AWS Organizations é um serviço global com um único endpoint, que funciona a partir de qualquer Regiões da AWS. Não é necessário selecionar explicitamente uma região na qual operar.

A replicação de dados que é por fim consistente

O AWS Organizations, como muitos outros serviços da AWS, é eventualmente consistente. O AWS Organizations atinge alta disponibilidade replicando dados entre vários servidores nos datacenters da AWS nesta região. Se uma solicitação para alterar alguns dados for bem-sucedida, a alteração estará comprometida e armazenada com segurança. No entanto, a alteração deve ser replicada em vários servidores. Para mais informações, consulte As alterações que eu faço nem sempre ficam imediatamente visíveis.

Uso gratuito

O AWS Organizations é um recurso da sua Conta da AWS oferecido gratuitamente. Você só é cobrado quando acessa outros serviços da AWS a partir das contas de sua organização. Para obter informações sobre preços de outros produtos da AWS, consulte a página de preços da Amazon Web Services.

## AWS OrganizationsDefinição de preço do

O AWS Organizations é oferecido sem custo adicional. Você será cobrado apenas pelos recursos da AWS que os usuários e as funções nas suas contas-membro usarem. Por exemplo, são cobradas as tarifas padrão para as instâncias do Amazon EC2 usadas pelos usuários ou pelas funções nas suas contas-membro. Para obter informações preços de outros serviços da AWS, consulte Preços da AWS.

## Como acessar o AWS Organizations

Você pode trabalhar com o AWS Organizations de qualquer uma das seguintes formas:

AWS Management Console

O AWS Organizations console é uma interface baseada em navegador que você pode usar para gerenciar sua organização e seus recursos da AWS. Você pode executar qualquer tarefa da sua organização usando o console.

AWS Ferramentas de linha de comando

Você pode usar as ferramentas de linha de comando da AWS para emitir comandos na linha de comando do sistema e realizar tarefas do AWS Organizations e da AWS. Usar a linha de comando pode ser mais rápido e mais conveniente do que o console. As ferramentas da linha de comando também são úteis se você quiser criar scripts que realizem tarefas da AWS.

A AWS fornece dois conjuntos de ferramentas de linha de comando:

- AWS Command Line Interface (AWS CLI). Para obter informações sobre a instalação e o uso da AWS CLI, consulte o Manual do usuário do AWS Command Line Interface.
- AWS Tools for Windows PowerShell. Para obter informações sobre a instalação e o uso do Tools for Windows PowerShell, consulte o Manual do usuário do AWS Tools for Windows PowerShell.

AWS SDKs

O SDKs da AWS consistem em bibliotecas e código de exemplo de várias linguagens de programação e plataformas (como Java, Python, Ruby, .NET, iOS e Android). Os SDKs processam tarefas como assinatura criptográfica de solicitações, gerenciamento de erros e novas tentativas automáticas de solicitações. Para obter mais informações sobre os SDKs da AWS, incluindo como fazer download deles e instalá-los, consulte Ferramentas da Amazon Web Services.

AWS Organizations API de consulta HTTPS

A API de consulta HTTPS do AWS Organizations proporciona acesso programático ao AWS Organizations e ao 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 Chamada de API fazendo solicitações de consulta HTTP e Referência da API do AWS Organizations.

# Suporte e comentários para o AWS Organizations

Os seus comentários são bem-vindos. Você pode enviar seus comentários para feedback-awsorganizations@amazon.com. Você também pode publicar seus comentários e perguntas no nosso AWS Organizations fórum de suporte. Para obter mais informações sobre os fóruns de suporte da AWS, consulte Ajuda com os fóruns.

# Outros recursos da AWS

- Cursos e treinamento da AWS – Links para cursos baseados em funções e especialidades, além de laboratórios autoguiados para ajudar a aprimorar suas habilidades em AWS e ganhar experiência prática.
- Ferramentas de desenvolvedor da AWS – Links para ferramentas de desenvolvedor e recursos que fornecem documentação, exemplos de código, notas de release e outras informações para ajudar você a desenvolver aplicativos inovadores com a AWS.
- Centro de suporte da AWS Support – A central para criar e gerenciar seus casos do AWS Support. Também inclui links para outros recursos úteis, como fóruns, perguntas frequentes, status de integridade do serviço e AWS Trusted Advisor.
- AWS Support – A principal página da Web para obter informações sobre o AWS Support, um canal de suporte de resposta rápida e com atendimento individual para ajudar a criar e executar aplicativos na nuvem.
- Entrar em contato – Um ponto central de contato para consultas relativas a faturas da AWS, contas, eventos, uso abusivo e outros problemas.
- Termos do site da AWS: informações detalhadas sobre nossos direitos autorais e marca registrada; sua conta, licença e acesso ao site, entre outros tópicos.

# Conceitos básicos do AWS Organizations

Os tópicos a seguir fornecem informações para ajudá-lo a começar a aprender e usar o AWS Organizations.

## Saiba mais sobre...

Terminologia e conceitos do AWS Organizations

Conheça a terminologia e os principais conceitos necessários para compreender AWS Organizations. Esta seção descreve cada um dos componentes de uma organização e os conceitos básicos de como eles funcionam em conjunto para fornecer um novo nível de controle sobre o que os usuários dessas contas podem fazer.

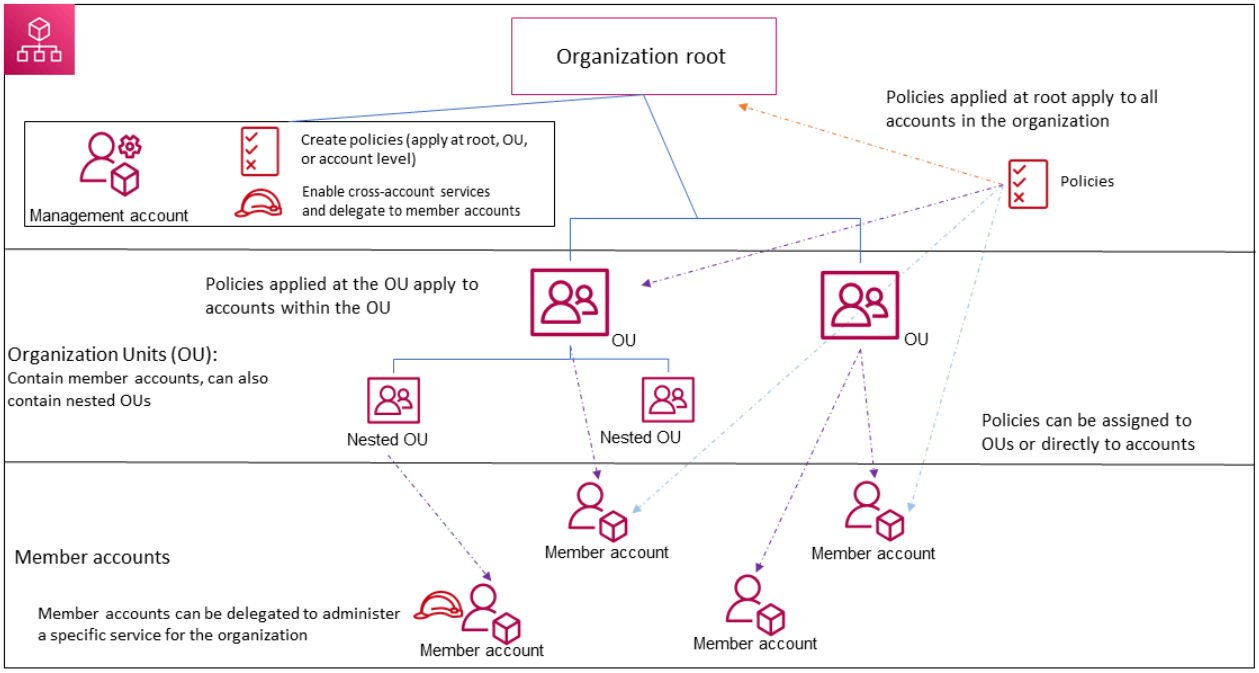
Faturamento consolidado para organizações

Um dos principais recursos sobre AWS Organizations é a consolidação do faturamento de todas as contas em sua organização. Saiba mais sobre como o faturamento será manipulado em uma organização e como vários descontos funcionam quando compartilhados entre várias contas. Esse conteúdo encontra-se no Manual do usuário do AWS Billing.

## Terminologia e conceitos do AWS Organizations

Para ajudá-lo a começar a usar o AWS Organizations, este tópico explica alguns dos conceitos-chave.

O diagrama a seguir mostra uma organização básica que consiste em cinco contas que estão organizadas em quatro unidades organizacionais (UOs) na raiz. A organização também tem várias políticas que são anexadas a algumas das UOs ou diretamente a contas. Para obter uma descrição de cada um desses itens, consulte as definições neste tópico.




Organização

Uma entidade que você cria para consolidar suas contas da AWS para poder administrá-las como uma só unidade. Você pode usar o AWS Organizations console para visualizar e gerenciar centralmente todas as suas contas dentro da sua organização. Uma organização tem uma conta de gerenciamento primária com zero ou mais contas-membro. É possível organizar as contas em uma estrutura em árvore hierárquica, com uma raiz na parte superior e unidades organizacionais aninhadas na raiz. Cada conta pode estar diretamente na raiz ou ser colocada em uma das UOs na hierarquia. Uma organização tem a funcionalidade que é determinada pelo conjunto de recursos que você ativar.

Raiz

O contêiner pai de todas as contas da sua organização. Se você aplicar uma política à raiz, ela será aplicada a todas as unidades organizacionais (UOs) e contas na organização.

> **Note**
>
> No momento, você pode ter apenas uma raiz. O AWS Organizations cria a raiz automaticamente para você quando uma organização é criada.

Unidade organizacional (UO)

Um contêiner para contas em uma raiz. Uma UO também pode conter outras UOs, permitindo que você crie uma hierarquia parecida com uma árvore de cabeça para baixo, com a raiz na parte superior e ramificações de UOs que se propagam para níveis inferiores, terminando em contas que são as folhas da árvore. Quando você anexa uma política a um dos nós na hierarquia, ele é propagado e afeta todas as ramificações (UOs) e folhas (contas) nos níveis inferiores. Uma UO pode ter exatamente um pai, e, atualmente, cada conta pode ser um membro de exatamente uma UO.

Conta

Uma conta em Organizations é uma Conta da AWS padrão que contém os seus recursos da AWS e as identidades que podem acessar esses recursos.

> **Tip**
>
> Uma conta da AWS não é o mesmo que uma conta de usuário. Um usuário AWS é uma identidade que você cria usando o AWS Identity and Access Management (IAM) que toma a forma de um usuário do IAM com credenciais de longo prazo ou uma função do IAM com credenciais de curto prazo. Uma única conta AWS pode conter, e normalmente contém, muitos usuários e funções.

Há dois tipos de contas em uma organização: uma única conta designada como conta de gerenciamento e uma ou mais contas-membro.

- A conta de gerenciamento é a conta que você usa para criar a organização. Na conta de gerenciamento da organização, é possível fazer o seguinte:
  - Criar contas na organização
  - Convidar outras contas existentes para a organização
  - Remover contas da organização
  - Designar contas de administrador delegado
  - Gerenciar convites
  - Aplicar políticas a entidades (raízes, UOs ou contas) dentro da organização
  - Habilitar a integração com os serviços compatíveis da AWS para fornecer a funcionalidade do serviço em todas as contas da organização.

A conta de gerenciamento tem as responsabilidades de uma conta pagadora e é responsável pelo pagamento de todos as cobranças que são acumuladas pelas contas-membro. Não é possível alterar a conta de gerenciamento de uma organização.

- As contas-membro compõem todo o resto das contas em uma organização. Uma conta da só pode ser membro de uma organização de cada vez. Você pode anexar uma política a uma conta para aplicar controles a apenas uma única conta.

> **Note**
>
> Você pode designar algumas contas-membro para serem contas de administrador delegado. Consulte Administrador delegado abaixo.

Administrador delegado

Recomendamos usar a conta de gerenciamento do Organizations e seus usuários e perfis somente para as tarefas que só podem ser executadas por essa conta. Além disso, recomendamos armazenar todos os seus recursos da AWS em outras contas-membro na organização e mantê-las fora da conta de gerenciamento. Isso porque os recursos de segurança, como as políticas de controle de serviços (SCPs) do Organizations, não restringem usuários ou perfis na conta de gerenciamento. Separar seus recursos da sua conta de gerenciamento também pode ajudar a entender os lançamentos em suas faturas. Na conta de gerenciamento da organização, é possível designar uma ou mais contas-membro como uma conta de administrador delegado para obter ajuda para implementar essa recomendação. Há dois tipos de administradores delegados:

- Administrador delegado do Organizations: essas contas permitem gerenciar as políticas da organização e anexar políticas às entidades (raízes, OUs ou contas) dentro da organização. A conta de gerenciamento pode controlar as permissões de delegação em níveis granulares. Consulte Administrador delegado para AWS Organizations para obter mais informações.
- Administrador delegado de um serviço da AWS: essas contas permitem gerenciar serviços da AWS que se integram às organizações. A conta de gerenciamento pode registrar diferentes contas-membro como administradores delegados para diferentes serviços, conforme necessário. Essas contas têm permissões administrativas para um serviço específico, bem como permissões para ações somente leitura do Organizations. Consulte Administrador delegado para serviços da AWS que funcionam com o Organizations para obter mais informações.

Convite

O processo para pedir que outra conta se inscreva na sua organização. Um convite só pode ser emitido pela conta de gerenciamento da organização. O convite é estendido para o ID da conta ou para o endereço de e-mail associado à conta convidada. Após a conta convidada aceitar um convite, ela se torna uma conta-membro na organização. Os convites também podem ser enviados a todas as contas-membro atuais quando a organização precisa que todos os membros aprovem a alteração de oferecer suporte apenas a recursos de faturamento consolidado para oferecer suporte a todos os recursos na organização. Os convites funcionam com a troca de handshakes das contas. Talvez você não veja handshakes quando trabalha no console do AWS Organizations. Mas se você usar a AWS CLI ou a API do AWS Organizations, deverá trabalhar diretamente com handshakes.

Handshake

Um processo de várias etapas de troca de informações entre duas partes. Um de seus usos principais no AWS Organizations é servir como a implementação subjacente de convites. As mensagens de handshake são transmitidas entre o iniciador de handshake e o destinatário e respondidas por eles. As mensagens são transmitidas de uma forma que ajuda ambas as partes a saber sempre qual é o status atual. Handshakes também são usados ao alterar a organização de oferecer suporte apenas a recursos de faturamento consolidado para oferecer suporte a todos os recursos disponibilizados pelo AWS Organizations. Você geralmente precisará interagir diretamente com handshakes somente se trabalhar com a API do AWS Organizations ou ferramentas da linha de comando, como a AWS CLI.

Conjuntos de recursos disponíveis

- Todos os recursos – O conjunto de recursos padrão que está disponível para o AWS Organizations. Inclui toda a funcionalidade do faturamento consolidado, além de recursos avançados que oferecem maior controle sobre as contas em sua organização. Por exemplo, quando todos os recursos estão habilitados, a conta de gerenciamento da organização tem controle total sobre o que as contas-membro podem fazer. A conta de gerenciamento pode aplicar SCPs para restringir os serviços e as ações que os usuários (incluindo o usuário-raiz) e as funções em uma conta podem acessar. A conta de gerenciamento também pode impedir que as contas-membro saiam da organização. É possível habilitar a integração com serviços compatíveis da AWS para permitir que esses serviços forneçam funcionalidades para todas as contas da organização.

Você pode criar uma organização com todos os recursos já habilitados, ou pode ativar todos os recursos em uma organização que originalmente oferecia suporte apenas aos recursos de faturamento consolidado. Para habilitar todos os recursos, todas as contas-membro convidadas devem aprovar a alteração aceitando o convite enviado quando a conta de gerenciamento inicia o processo.

- Faturamento consolidado: esse conjunto de recursos fornece a funcionalidade de cobrança compartilhada, mas não inclui os recursos mais avançados do AWS Organizations. Por exemplo, não é possível habilitar outros serviços da AWS para integração com sua organização e fazê-lo funcionar em todas as suas contas, ou usar políticas para restringir o que usuários e perfis em contas diferentes podem fazer. Para usar os recursos avançados do AWS Organizations, habilite todos os recursos em sua organização.

Política de controle de serviço (SCP - service control policy)

Uma política que especifica os serviços e as ações que os usuários e as funções podem usar nas contas que o SCP afeta. As SCPs são semelhantes às políticas de permissão do IAM, exceto por não concederem permissões. Em vez disso, as SCPs especificam o máximo de permissões para uma organização, unidade organizacional (UO) ou conta. Quando você anexa uma SCP à sua organização raiz ou a uma UO, a SCP limita as permissões a entidades em contas-membro.

Listas de permissões versus listas de negações

Listas de permissões e listas de negações são estratégias complementares que você pode usar para aplicar SCPs para filtrar as permissões disponíveis para as contas.

- Estratégia de lista de permissões – Você especifica explicitamente o acesso que é permitido. Todos os outros acessos são bloqueados implicitamente. Por padrão, o AWS Organizations anexa uma política gerenciada pela AWS denominada `FullAWSAccess` a todas as raízes, UOs e contas. Isso ajuda a garantir que, à medida que você desenvolve sua organização, nada fica bloqueado até você querer que seja. Em outras palavras, por padrão, todas as permissões são concedidas. Quando você estiver pronto para restringir permissões, substitua a política `FullAWSAccess` por uma que permita apenas o conjunto de permissões desejado e mais limitado. Os usuários e funções nas contas afetadas podem exercer apenas esse nível de acesso, mesmo que as políticas do IAM correspondentes permitam todas as ações. Se substituir a política padrão na raiz, todas as contas na organização serão afetadas pelas restrições. Não é possível adicionar as permissões de volta em um nível inferior na hierarquia porque uma SCP nunca concede permissões; ela apenas as filtra.

- Estratégia de lista de negação: você especifica explicitamente o acesso que não é permitido. Todos os outros acessos são permitidos. Nesse cenário, todas as permissões são permitidas, a menos que explicitamente bloqueadas. Esse é o comportamento padrão do AWS Organizations. Por padrão, o AWS Organizations anexa uma política gerenciada pela AWS denominada `FullAWSAccess` a todas as raízes, UOs e contas. Isso permite que qualquer conta acesse qualquer serviço ou operação sem nenhuma restrição imposta pelo AWS Organizations Ao contrário da técnica de lista de permissões descrita acima, ao usar listas de negação, você deixa a política `FullAWSAccess` padrão no lugar (que permite “todos”). Mas, em seguida, você anexa políticas adicionais que negam explicitamente o acesso aos serviços e ações indesejados. Assim como acontece com as políticas de permissão do IAM,,. uma negação explícita de uma ação de serviço substitui qualquer permissão dessa ação.

Política de exclusão de serviços de inteligência artificial (IA)

Um tipo de política que ajuda você a padronizar suas configurações de exclusão para serviços de IA da AWS em todas as contas de sua organização. Certos serviços de IA da AWS podem armazenar e usar conteúdo de clientes processado por esses serviços para o desenvolvimento e a melhoria contínua dos serviços e tecnologias de IA da Amazon. Como um cliente da AWS, você pode usar as Políticas de exclusão de serviço de IA para optar por não ter o seu conteúdo armazenado nem utilizado para melhorias no serviço.

Política de backup

Um tipo de política que ajuda a padronizar e implementar uma estratégia de backup para os recursos de todas as contas de sua organização. Em um política de backup, você pode configurar e implantar planos de backup para seus recursos.

Política de tag

Um tipo de política que ajuda a padronizar tags em todos os recursos de todas as contas da organização. Em uma política de tag, você pode especificar regras de atribuição de tags para recursos específicos.

# Tutoriais do AWS Organizations

Use os tutoriais nesta seção para saber como executar tarefas usando o AWS Organizations.

Tutorial: criar e configurar uma organização

Comece a trabalhar com instruções passo a passo para criar sua organização, convidar suas primeiras contas-membro, criar uma hierarquia UO que contenha suas contas e aplicar algumas políticas de controle de serviço (SCPs).

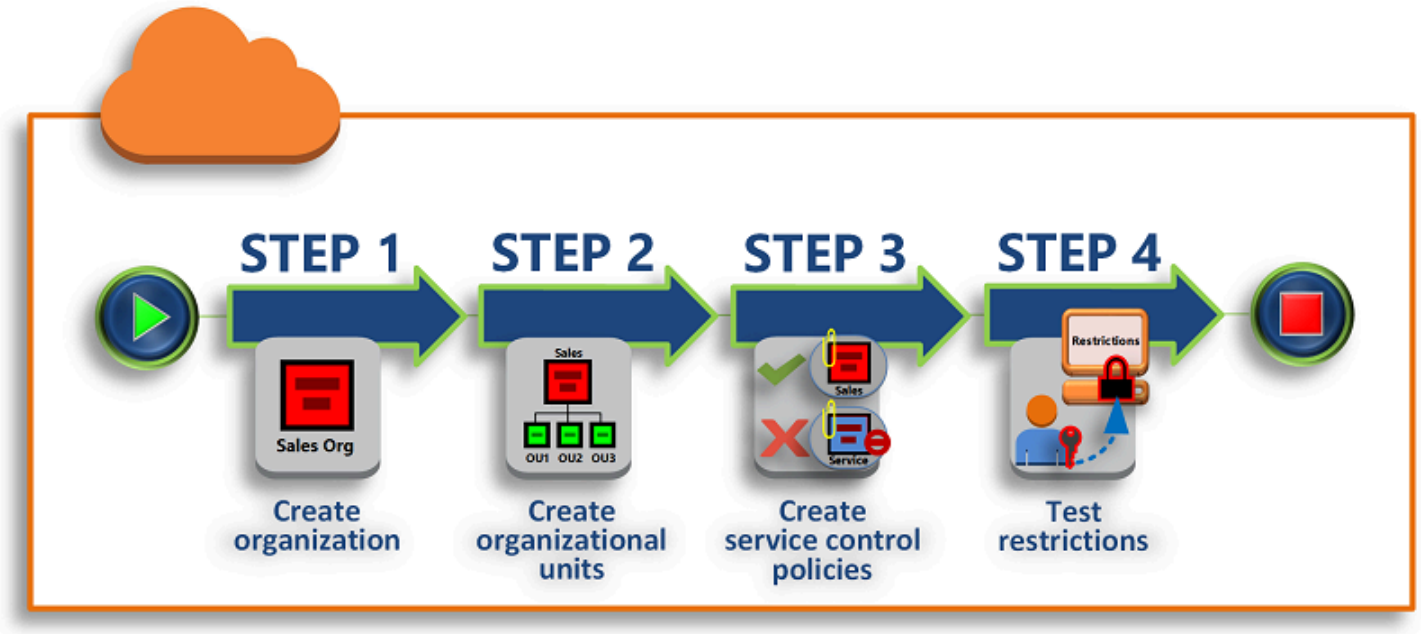
Tutorial: monitorar alterações importantes em sua organização com o Amazon EventBridge

Monitore as principais alterações em sua organização configurando o Amazon EventBridge para disparar um alarme em forma de e-mail, mensagem de texto SMS ou entrada de log quando as ações que você designar ocorrerem em sua organização. Por exemplo, muitas organizações querem saber quando uma nova conta é criada ou quando uma conta tenta deixar a organização.

## Tutorial: criar e configurar uma organização

Neste tutorial, você cria sua organização e configurá-lo com duas contas-membro da AWS. Você cria uma das contas-membro em sua organização e convida outras contas para a inscrição da sua organização. Depois, você usa a técnica de lista de permissões para especificar que os administradores podem delegar apenas os serviços e ações listados explicitamente. Isso permite que os administradores validem qualquer novo serviço apresentado pela AWS antes de permitir o seu uso por outra pessoa em sua empresa. Dessa forma, se a AWS apresentar um novo serviço, ele permanecerá proibido até que um administrador adicione o serviço à lista de permissões na política adequada. O tutorial também mostra como usar a lista de negações para garantir que nenhum usuário em uma conta-membro possa alterar a configuração dos logs de auditoria criados pelo AWS CloudTrail.

A seguinte ilustração mostra as etapas principais do tutorial.




### Etapa 1: criar sua organização

Nesta etapa, você cria uma organização com sua Conta da AWS atual como a conta de gerenciamento. Você também pode convidar uma Conta da AWS para participar da sua organização e criar uma segunda conta como uma conta-membro.

### Etapa 2: criar as unidades organizacionais

Em seguida, você cria duas unidades organizacionais (UOs) na sua nova organização e coloca a conta-membro nestas UOs.

### Etapa 3: criar as políticas de controle de serviço

É possível aplicar restrições às ações que podem ser delegadas para usuários e funções nas contas-membro usando políticas de controle de serviço (SCPs). Nesta etapa, você cria duas SCPs e anexa-as às UOs de sua organização.

### Etapa 4: testar suas políticas da organização

Você pode fazer login como usuários de cada uma das contas de teste e ver os efeitos que as SCPs têm sobre as contas.

Nenhuma das etapas deste tutorial incorrem em custos em sua fatura da AWS. O AWS Organizations é um serviço gratuito.

## Pré-requisitos

Este tutorial pressupõe que você tenha acesso e possa fazer login em duas Contas da AWS existentes (você cria uma terceira como parte deste tutorial) e que possa fazer login em ambas como administrador.

O tutorial refere-se às contas como o seguinte:

- `111111111111` – a conta que você usa para criar a organização. Esta conta torna-se a conta de gerenciamento. O proprietário desta conta tem um endereço de e-mail do `OrgAccount111@example.com`.
- `222222222222` – uma conta que você convida para participar da organização como conta-membro. O proprietário desta conta tem um endereço de e-mail do `member222@example.com`.
- `333333333333` – uma conta que você cria como um membro da organização. O proprietário desta conta tem um endereço de e-mail do `member333@example.com`.

Substitua os valores acima pelos valores associados às suas contas de teste. Recomendamos não usar contas de produção para este tutorial.

## Etapa 1: criar sua organização

Nesta etapa, você faz login na conta 111111111111 como administrador, cria uma organização com essa conta como conta de gerenciamento e convida uma conta existente, 222222222222, para participar como uma conta-membro.

AWS Management Console

1. Faça login no AWS como administrador na conta 111111111111 e abra o console do AWS Organizations.
2. Na página de introdução, escolha Create an organization (Criar uma organização).
3. Na caixa de diálogo de confirmação, escolha Create Organization (Criar uma organização).

> **Note**
>
> Por padrão, a organização é criada com todos os recursos habilitados. Você também pode criar a organização apenas com recursos de faturamento consolidado habilitados.

A AWS cria a organização e exibe a página Contas da AWS para você. Se você estiver em uma página diferente, escolha Contas da AWS no painel de navegação à esquerda.

Se a conta que você usa nunca teve seu endereço de e-mail verificado pela AWS, um e-mail de verificação é enviado automaticamente para o endereço associado à sua conta de gerenciamento. Talvez haja um atraso até você receber o e-mail de verificação.

4. Verifique o endereço de e-mail em 24 horas. Para obter mais informações, consulte Verificação do endereço de e-mail.

Você agora tem uma organização que tem sua conta como o único membro. Esta é a conta de gerenciamento da organização.

## Convide uma conta atual para participar da sua organização

Agora que você tem uma organização, você pode começar a preenchê-la com contas. Nas etapas nesta seção, você convida uma conta existente para participar e se tornar um membro da sua organização.

AWS Management Console

Para convidar uma conta existente para participar

1. Navegue até a página Contas da AWS e escolha Add an Conta da AWS (Adicionar uma Conta da AWS).
2. Na página Adicionar uma Conta da AWS), escolha Convidar uma Conta da AWS existente.
3. Na caixa Endereço de e-mail ou ID de uma Conta da AWS a ser convidada, insira o endereço de e-mail do proprietário da conta que você deseja convidar, de forma semelhante ao seguinte: **`member222@example.com`**. Alternativamente, se souber o número do ID da Conta da AWS, você pode inseri-lo em vez disso.
4. Digite o texto que você deseja na caixa Message to include in the invitation email message (Mensagem a ser incluída na mensagem de e-mail do convite). Esse texto é incluído no e-mail que é enviado para o proprietário da conta.
5. Escolha Send invitation (Enviar convite). A AWS Organizations envia o convite para o proprietário da conta.

> **Important**
>
> Expanda a mensagem de erro, se indicado. Se o erro indicar que você excedeu os limites da sua conta para a organização ou que não é possível adicionar uma conta porque sua organização ainda está inicializando, aguarde até uma hora depois de criar a organização e tente novamente. Se o erro persistir, entre em contato com o AWS Support.

6. Para os fins deste tutorial, você agora precisa aceitar seu próprio convite. Execute uma das seguintes ações para acessar a página Convites no console:

   - Abra o e-mail enviado pela AWS da conta de gerenciamento e escolha o link para aceitar o convite. Quando solicitado a fazer login, faça isso como um administrador na conta-membro convidada.
   - Abra o console do AWS Organizations e navegue até a página de Invitations (Convites).

7. Na página Contas da AWS, escolha Accept (Aceitar) e depois Confirm (Confirmar).

   > **Tip**
   >
   > O recebimento do convite pode demorar e, talvez, você precise aguardar para aceitar o convite.

8. Saia da sua conta-membro e faça login novamente como um administrador na sua conta de gerenciamento.

## Crie uma conta-membro

Nas etapas desta seção, você cria uma Conta da AWS que é automaticamente um membro da organização. Chamamos essa conta no tutorial de 333333333333.

AWS Management Console

Para criar uma conta-membro

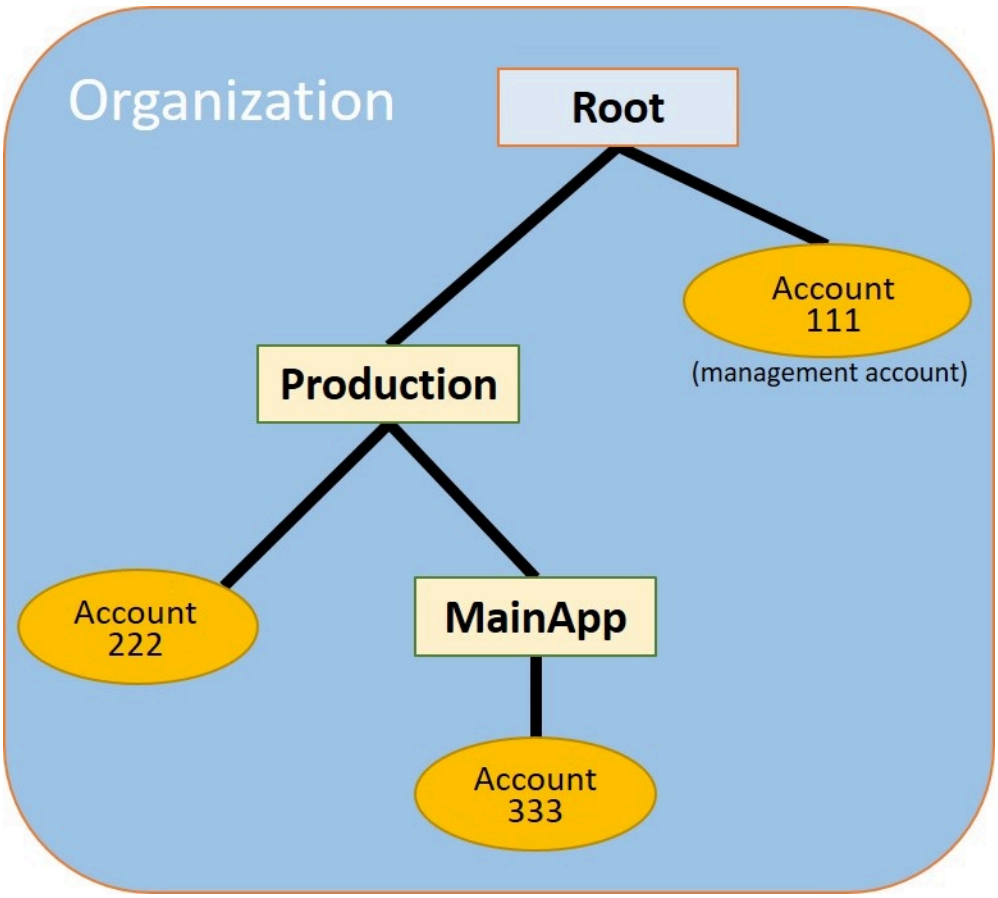
1. No console do AWS Organizations, na página Contas da AWS, escolha Adicionar Conta da AWS.
2. Na página Adicionar umaConta da AWS, escolha Criar uma Conta da AWS.

3. Em Nome da Conta da AWS, insira um nome para a conta, por exemplo, **`MainApp Account`**.
4. Em Email address of the account's root user (Endereço de e-mail do usuário da conta-raiz), digite o endereço de e-mail da pessoa que deve receber comunicações em nome da conta. Esse valor deve ser exclusivo globalmente. Não é possível que duas contas tenham o mesmo endereço de e-mail. Por exemplo, convém usar algo como **`mainapp@example.com`**.
5. Para Nome da função do IAM, você pode deixar isso em branco para usar automaticamente o nome da função padrão do `OrganizationAccountAccessRole` ou você pode fornecer o seu próprio nome. Essa função permite acessar a nova conta-membro quando conectado como um usuário do IAM na conta de gerenciamento. Para este tutorial, deixe em branco para instruir o AWS Organizations a criar a função com o nome padrão.
6. Escolha CriarConta da AWS. Você pode precisar esperar um pouco e, ao mesmo tempo, atualizar a página para a nova conta aparecer na página Contas da AWS.

> **Important**
>
> Se você receber um erro que indica que excedeu seus limites de conta para a organização ou que não pode adicionar uma conta porque sua organização ainda está inicializando, aguarde uma hora depois de criar a organização e tente novamente. Se o erro persistir, entre em contato com o AWS Support.

## Etapa 2: criar as unidades organizacionais

Nas etapas desta seção, você cria unidades organizacionais (UOs) e coloca suas contas-membro. Quando terminar, a hierarquia será semelhante à seguinte ilustração. A conta de gerenciamento permanece na raiz. Uma conta-membro é movida para a UO de produção e a outra é movida para a UO MainApp, que é um filho de produção.




AWS Management Console

Para criar e preencher as UOs

> **Note**
>
> Nas etapas a seguir, você interage com objetos para os quais pode escolher o nome do próprio objeto ou o botão de opção ao lado do objeto.
>
> - Se escolher o nome do objeto, você abre uma nova página que exibe os detalhes dos objetos.
> - Se escolher o botão de opção ao lado do objeto, você estará identificando esse objeto para ser objeto de outra ação, como escolher uma opção de menu.
>
> As etapas a seguir fazem com que você escolha o botão de opção para que possa agir sobre o objeto associado fazendo escolhas de menu.

1. No console do AWS Organizations navegue até a página Contas da AWS.
2. Escolha a caixa de seleção
   
   ao lado do contêiner Raiz.
3. Na guia Children (Subordinadas), escolha Actions (Ações) e, depois, em Organizational unit (Unidade organizacional), escolha Create new (Criar nova).
4. Na página Create organizational unit in Root (Criar unidade organizacional na raiz), para o Create organizational unit in Root (Nome da unidade organizacional), insira **`Production`** e, depois, escolha Create organizational unit (Criar unidade organizacional).
5. Escolha a caixa de seleção
   
   ao lado da nova UO de Produção.
6. Selecione Actions (Ações), depois, em Organizational unit (Unidade organizacional), escolha Create new (Criar nova).
7. Na página Create organizational unit in Root (Criar unidade organizacional na raiz), para o nome da segunda UO, insira **`MainApp`** e, depois, escolha Create organizational unit (Criar unidade organizacional).

   Agora você pode mover suas contas-membro para essas UOs.
8. Retorne para a página Contas da AWS e expanda a árvore em sua UO Production (Produção) escolhendo o triângulo
   
   ao lado dela. Isso exibe a UO MainApp como subordinada de Produção.
9. Ao lado de 333333333333, marque a caixa de seleção
   
   (não o nome dela), escolha Actions (Ações) e, em Conta da AWS, escolha Move (Mover).
10. Na página Move Conta da AWS '333333333333' (Mover conta da AWS ‘333333333333’), escolha o triângulo ao lado de Production (Produção) para expandi-lo. Ao lado de MainApp, escolha o botão de rádio
    
    (não o nome dele), em seguida escolha Move Conta da AWS (Mover conta da AWS).
11. Ao lado de 222222222222, marque a caixa de seleção
    
    (não o nome dela), escolha Actions (Ações) e, em Conta da AWS, escolha Move (Mover).

12. Na página Move Conta da AWS ‘222222222222’ (Mover conta da AWS ‘222222222222’), ao lado de Production (Produção), escolha o botão de rádio (não o nome dele), em seguida escolha Move Conta da AWS (Mover conta da AWS).

## Etapa 3: criar as políticas de controle de serviço

Nas etapas desta seção, você cria três políticas de controle de serviço (SCPs) e anexa-as à raiz e às UOs para restringir o que os usuários podem fazer nas contas da organização. A primeira SCP impede que qualquer pessoa em qualquer uma das contas-membro crie ou modifique quaisquer logs do AWS CloudTrail que você configurar. A conta de gerenciamento não é afetada por qualquer SCP, portanto, depois de aplicar a SCP do CloudTrail, você deve criar todos os logs na conta de gerenciamento.

### Habilitar o tipo de política de controle de serviço para a organização

Para poder anexar uma política de qualquer tipo a uma raiz ou a qualquer O em uma raiz, você deve habilitar o tipo de política para a organização. Os tipos de política não estão habilitados por padrão. As etapas desta seção mostram como habilitar o tipo de política de controle de serviço (SCP) para sua organização.

AWS Management Console

Para habilitar SCPs para a organização

1. Navegue até a página Policies (Políticas) e escolha Service control policies (Políticas de controle de serviço).
2. Na página Service Control Policies (Políticas de controle de serviço), escolha Enable service control policies (Ativar políticas de controle de serviço).

   Um banner verde é exibido para informar que agora você pode criar SCPs em sua organização.

### Criar suas SCPs

Agora que as políticas de controle de serviço estão habilitadas em sua organização, você pode criar as três políticas necessárias para este tutorial.

AWS Management Console

Para criar a primeira SCP que bloqueia as ações de configuração do CloudTrail

1. Navegue até a página Policies (Políticas) e escolha Service control policies (Políticas de controle de serviço).
2. Na página Service control policies (Políticas de controle de serviço), escolha Create policy (Criar política).
3. Em Nome da política, insira **`Block CloudTrail Configuration Actions`**.
4. Na seção Policy (Política), na lista de serviços à direita, selecione CloudTrail para o serviço. Depois escolha as seguintes ações: AddTags, CreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging e UpdateTrail.
5. Ainda no painel direito, escolha Add resource (Adicionar recurso) e especifique CloudTrail e All Resources (Todos os recursos). Escolha Add resource (Adicionar recurso).

   A instrução de política à esquerda deve ser semelhante ao seguinte exemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Escolha Criar política.

A segunda política define uma lista de permissões de todos os serviços e ações que você deseja habilitar para usuários e funções na UO de produção. Depois de você concluir, os usuários na UO de produção poderão acessar apenas os serviços e ações listados.

AWS Management Console

Como criar a segunda política que permite serviços aprovados para a UO de produção

1. Na página Service control policies (Políticas de controle de serviço), escolha Create policy (Criar política).
2. Em Nome da política, insira **`Allow List for All Approved Services`**.
3. Posicione o cursor no painel à direita da seção Policy (Política) e cole uma política como a seguinte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. Escolha Criar política.

A política final fornece uma lista de negações de serviços que são bloqueados para uso na UO MainApp. Para este tutorial, você bloqueia o acesso ao Amazon DynamoDB em todas as contas que estão na UO MainApp.

AWS Management Console

Como criar a terceira política que nega o acesso a serviços que não podem ser usados na UO MainApp

1. Na página Service control policies (Políticas de controle de serviço), escolha Create policy (Criar política).
2. Em Nome da política, insira **`Deny List for MainApp Prohibited Services`**.
3. Na seção Policy (Política) à esquerda, selecione Amazon DynamoDB para o serviço. Para a ação, escolha All actions (Todas as ações).
4. Ainda no painel esquerdo, selecione Add resource (Adicionar recurso) e especifique DynamoDB e All Resources (Todos os recursos). Escolha Add resource (Adicionar recurso).

   A instrução de política à direita é atualizada para ser semelhante ao seguinte.

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Deny",
         "Action": [ "dynamodb:*" ],
         "Resource": [ "*" ]
       }
     ]
   }
   ```

5. Escolha Create policy (Criar política) para salvar a SCP.

## Anexe as SCPs às suas UOs

Agora que as SCPs existem e estão habilitadas para a raiz, você pode anexá-las para a raiz e UO.

AWS Management Console

Para anexar as políticas à raiz e às UOs

1. Navegue até o página Contas da AWS.
2. Na página Contas da AWS, escolha Root (Raiz) (seu nome, não o botão de opção) para navegar até a respectiva página de detalhes.

3. Na página de detalhes de Root (Raiz), a guia Policies (Políticas) e, em Service Control Policies (Políticas de controle de serviço), escolha Attach (Anexar).
4. Na página Attach a service control policy (Anexar política de controle de serviço), escolha o botão de seleção ao lado da SCP chamada `Block CloudTrail Configuration Actions`, depois, escolha Attach (Anexar). Neste tutorial, você anexa-a à raiz para que afete todas as contas-membro para impedir que alguém altere sua configuração do CloudTrail.

   Na página de detalhes de Raiz, a guia Policies (Políticas) agora mostra que duas SCPs estão anexadas à raiz: a que você acabou de anexar e a SCP padrão `FullAWSAccess`.
5. Navegue novamente para a página Contas da AWS e escolha a UO Production (Produção) (o nome, não o botão de opção) para navegar até a respectiva página de detalhes.
6. Na página de detalhes da UO Produção, escolha a guia Policies (Políticas).
7. Em Service Control Policies (Políticas de controle de serviço), escolha Attach (Anexar).
8. Na página Attach a service control policy (Anexar política de controle de serviço), escolha o botão de seleção ao lado de `Allow List for All Approved Services`, depois, escolha Attach (Anexar). Isso permite que os usuários ou funções das contas-membro na UO Produção acessem os serviços aprovados.
9. Escolha a guia Policies (Políticas) novamente para ver que duas SCPs estão anexadas à UO: a que você acabou de anexar e a SCP padrão `FullAWSAccess`. No entanto, como a SCP `FullAWSAccess` também é uma lista de autorização que permite todos os serviços e ações, você deve desvincular essa SCP para garantir que apenas os serviços aprovados sejam permitidos.
10. Para remover a política padrão da UO Produção, escolha o botão de opção para FullAWSAccess, escolha Detach (Desvincular) e, na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

    Depois de remover essa política padrão, todas as contas-membro na UO Produção perdem imediatamente o acesso a todas as ações e os serviços que não estão na SCP de lista de permissões anexada na etapa anterior. Todas as solicitações para usar ações que não estão incluídas na SCP Allow List for All Approved Services (Lista de permissões para todos os serviços aprovados) são negadas. Isso é válido mesmo se um administrador de uma conta conceder acesso a outro serviço anexando uma política de permissões do IAM a um usuário em uma das contas-membro.

11. Agora você pode anexar a SCP chamada `Deny List for MainApp Prohibited services` para impedir que qualquer pessoa nas contas na UO do MainApp de usar quaisquer serviços restritos.

    Para fazer isso, navegue até a página Contas da AWS, escolha o ícone de triângulo para expandir a ramificação da UO Produção, depois, escolha a UO Production (Produção) e escolha MainApp (o nome, não o botão de opção) para navegar no respectivo conteúdo.
12. Na página de detalhes de MainApp, escolha a guia Policies (Políticas).
13. Em Service Control Policies (Políticas de controle de serviço), escolha Attach (Anexar) e, na lista de políticas disponíveis, escolha o botão de opção ao lado de Deny List for MainApp Prohibited Services (Lista de negação para serviços proibidos para MainApp), depois, escolha Attach policy (Anexar política).

## Etapa 4: testar suas políticas da organização

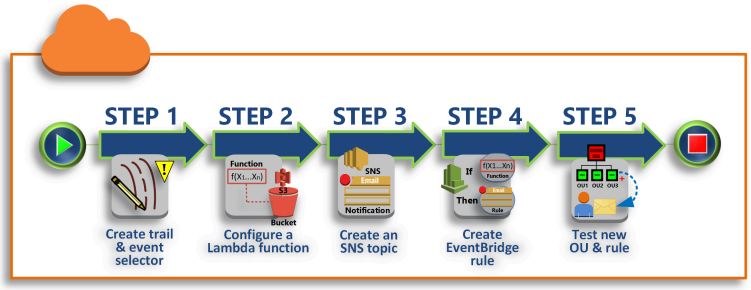
Agora é possível fazer login como usuário em qualquer uma das contas-membro e tentar executar várias ações da AWS:

- Se você fizer login como um usuário na conta de gerenciamento, poderá executar qualquer operação permitida por suas políticas de permissões do IAM. As SCPs não afetam nenhum usuário ou função da conta de gerenciamento, independentemente da raiz ou da UO em que a conta está localizada.
- Se fizer login como um usuário na conta 222222222222, você poderá executar qualquer ação permitida pela lista de permissões. O AWS Organizations nega qualquer tentativa de executar uma ação em qualquer serviço que não esteja na lista de permissões. Além disso, o AWS Organizations nega qualquer tentativa de executar uma das ações de configuração do CloudTrail.
- Se fizer login como usuário na conta 333333333333, você poderá executar qualquer ação permitida pela lista de permissões e não bloqueadas pela lista de negações. O AWS Organizations nega qualquer tentativa de executar uma ação que não esteja na política de lista de permissões e qualquer ação que esteja na política de lista de negações. Além disso, o AWS Organizations nega qualquer tentativa de executar uma das ações de configuração do CloudTrail.

# Tutorial: monitorar alterações importantes em sua organização com o Amazon EventBridge

Este tutorial mostra como configurar o Amazon EventBridge, anteriormente Amazon CloudWatch Events, para monitorar alterações em sua organização. Você começa por configurar uma regra que é acionada quando os usuários invocam operações específicas do AWS Organizations. Em seguida, você configura o Amazon EventBridge para executar uma função do AWS Lambda quando a regra é acionada e configura o Amazon SNS para enviar um e-mail com detalhes sobre o evento.

A seguinte ilustração mostra as etapas principais do tutorial.




[Etapa 1: configurar um seletor de eventos e trilhas](#)

Crie um log, chamado trilha, em AWS CloudTrail. Você configura-o para capturar todas as chamadas de API.

[Etapa 2: Configurar uma função do Lambda](#)

Crie uma função AWS Lambda que registra detalhes sobre o evento para um bucket do S3.

[Etapa 3: Criar um tópico do Amazon SNS que envia e-mails para assinantes](#)

Crie um tópico do Amazon SNS que envia e-mails para seus assinantes e, em seguida, inscreva-se no tópico.

[Etapa 4: criar uma regra do Amazon EventBridge](#)

Crie uma regra que diz ao Amazon EventBridge para passar detalhes de chamadas de API especificadas para a função do Lambda e para os assinantes do tópico do SNS.

[Etapa 5: testar sua regra do Amazon EventBridge](#)

Teste a sua nova regra executando uma das operações monitoradas. Neste tutorial, a operação monitorada é a criação de uma unidade organizacional (UO). Você vê a entrada do log que a função do Lambda cria e o e-mail que o Amazon SNS envia aos assinantes.

> **Dica**
>
> Você também poderá usar este tutorial como um guia para configurar operações semelhantes, como enviar notificações por e-mail quando a criação da conta estiver concluída. Como a criação da conta é uma operação assíncrona, por padrão, você não é notificado quando ela é concluída. Para obter mais informações sobre como usar o AWS CloudTrail e o Amazon EventBridge com o AWS Organizations, consulte Registrar em log e monitorar no AWS Organizations.

## Pré-requisitos

Este tutorial assume o seguinte:

- Você pode fazer login no AWS Management Console como um usuário do IAM da conta de gerenciamento de sua organização. O usuário do IAM deve ter permissões para criar e configurar um log no CloudTrail, uma função no Lambda, um tópico no Amazon SNS e uma regra no Amazon EventBridge. Para obter mais informações sobre a concessão de permissões, consulte Gerenciamento de acesso no Manual do usuário do IAM ou o guia do serviço para o qual você deseja configurar acesso.
- Você tem acesso a um bucket do Amazon Simple Storage Service (Amazon S3) (ou tem permissões para criar um bucket) para receber o log do CloudTrail que você configura na etapa 1.

> **Important**
>
> No momento, o AWS Organizations só é hospedado na região Leste dos EUA (Norte da Virgínia) (embora esteja disponível globalmente). Para executar as etapas neste tutorial, você deve configurar o AWS Management Console para usar essa região.

## Etapa 1: configurar um seletor de eventos e trilhas

Nesta etapa, você faz login na conta de gerenciamento e configura um log (chamado de trilha) no AWS CloudTrail. Você também configura um seletor de eventos na trilha para capturar todas as chamadas de API de leitura e gravação para que o Amazon EventBridge tenha chamadas para acionar.

Para criar uma trilha

1. Faça login na AWS como administrador da conta de gerenciamento da organização e abra o console do CloudTrail em https://console.aws.amazon.com/cloudtrail/.
2. Na barra de navegação no canto superior direito do console, escolha a região US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)). Se você escolher uma região diferente, o AWS Organizations não aparecerá como uma opção nas definições de configuração do Amazon EventBridge e o CloudTrail não capturará informações sobre o AWS Organizations.
3. No painel de navegação, selecione Trilhas.
4. Escolha Create Trail (Criar trilha).
5. Em Trail name (Nome da trilha), digite **`My-Test-Trail`**.
6. Execute uma das seguintes opções para especificar onde o CloudTrail deve entregar seus logs:
   - Se precisar criar um bucket, escolha Create new S3 bucket (Criar um novo bucket do S3) e, em Trail log bucket and folder (Bucket e pasta de log de trilha), insira um nome para o novo bucket.

     > **Note**
     >
     > Os nomes de buckets do S3 devem ser exclusivos globalmente.

   - Se você já tiver um bucket, escolha Use existing S3 bucket (Usar bucket do S3 existente) e, em seguida, escolha o nome do bucket na lista S3 bucket (Buckets do S3).
7. Escolha Next (Próximo).
8. Na página Choose log events (Escolher eventos de log), na seção Management events (Eventos de gerenciamento), escolha Read (Ler) e Write (Gravar).
9. Escolha Next (Próximo).
10. Verifique suas seleções e escolha Create trail (Criar trilha).

O Amazon EventBridge permite que você escolha entre diversas maneiras diferentes de enviar alertas quando uma regra de alarme corresponder a uma chamada de API recebida. Este tutorial demonstra dois métodos: invocar uma função do Lambda que pode registrar a chamada de API no log e enviar informações para um tópico do Amazon SNS que envia um e-mail ou mensagem de texto para os assinantes do tópico. Nas duas próximas etapas, você criará os componentes necessários: a função do Lambda e o tópico do Amazon SNS.

# Etapa 2: Configurar uma função do Lambda

Nesta etapa, você cria uma função do Lambda que registra em log a atividade da API enviada a ela pela regra do Amazon EventBridge configurada posteriormente.

Criar uma função do Lambda que registra em log eventos do Amazon EventBridge

1. Abra o console do AWS Lambda em https://console.aws.amazon.com/lambda/.
2. Se você não tiver familiaridade com o Lambda, escolha Get Started Now (Começar a usar agora) na página de boas-vindas. Caso contrário, escolha Create function (Criar função).
3. Na página Create function (Criar função), selecione Usar um blueprint (Usar um esquema).
4. Na caixa de pesquisa Blueprints (Esquemas), digite**`hello`** para o filtro e escolha o esquema hello-world.
5. Selecione Configurar.
6. Na página Basic information (Informações básicas), faça o seguinte:
   a. No nome da função do Lambda, insira **`LogOrganizationEvents`** na caixa de texto Name (Nome).
   b. Em Role (Função), escolha Create a new role with basic Lambda permissions (Criar uma nova função com permissões básicas do Lambda). Essa função concede à sua função do Lambda permissões para acessar os dados necessários e para gravar seu log de saída.
7. Edite o código da função do Lambda, conforme mostrado no exemplo a seguir.

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

   Este código de exemplo registra o evento em log com uma string do marcador **`LogOrganizationEvents`** seguida pela string JSON que compõe o evento.
8. Escolha Criar Função.

## Etapa 3: Criar um tópico do Amazon SNS que envia e-mails para assinantes

Nesta etapa, você cria um tópico do Amazon SNS que envia informações por e-mail a seus assinantes. Você torna esse tópico um destino da regra do Amazon EventBridge criada posteriormente.

Para criar um tópico do Amazon SNS para enviar um e-mail aos assinantes

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/.
2. No painel de navegação, escolha Topics (Tópicos).
3. Selecione Create new topic (Criar novo tópico).
    a. Em Topic name (Nome do tópico), digite **`OrganizationsCloudWatchTopic`**.
    b. Em Display name (Nome de exibição), digite **`OrgsCWEvnt`**.
    c. Escolha Criar tópico.
4. Agora você pode criar uma assinatura para o tópico. Escolha o ARN para o tópico que você acabou de criar.
5. Selecione Create subscription.
    a. Na página Create subscription (Criar assinatura), em Protocol (Protocolo), selecione Email (E-mail).
    b. Para Endpoint, insira seu endereço de e-mail.
    c. Escolha Create subscription (Criar assinatura). A AWS envia um e-mail ao endereço de e-mail que você especificou na etapa anterior. Aguarde até o e-mail chegar e, em seguida, clique no link Confirmar assinatura no e-mail para verificar se você recebeu o e-mail corretamente.
    d. Volte ao console e atualize a página. A mensagem Confirmação pendente desaparece e é substituída pelo ID de assinatura agora válido.

## Etapa 4: criar uma regra do Amazon EventBridge

Agora que a função do Lambda necessária existe em sua conta, você cria uma regra do Amazon EventBridge que a invoca quando os critérios da regra são atendidos.

Para criar uma regra de EventBridge

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Defina o console para a região US East (N. Virginia) (Leste dos EUA [Norte da Virgínia]) ou as informações sobre o Organizations não estarão disponíveis. Na barra de navegação no canto superior direito do console, escolha a região US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)).
3. Para obter instruções sobre como criar regras, consulte Getting started with Amazon EventBridge (Conceitos básicos do Amazon EventBridge) no guia do usuário do Amazon EventBridge.

## Etapa 5: testar sua regra do Amazon EventBridge

Nesta etapa, você cria uma unidade organizacional (UO) e acompanha a regra do Amazon EventBridge, gera uma entrada de log e envia um e-mail para si mesmo com detalhes sobre o evento.

AWS Management Console

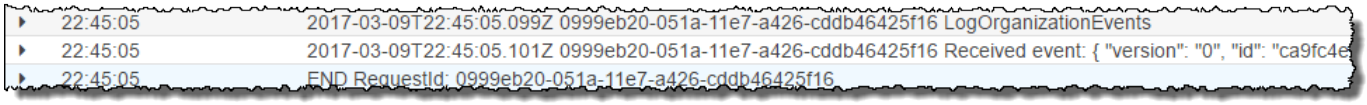
Para criar uma UO

1. Abra o console do AWS Organizations na página Contas da AWS
2. Escolha a caixa de seleção
   ☑
   Root OU (UO raiz), escolha Actions (Ações)e, em Organizational unit (Unidade organizacional), escolha Create (Criar).
3. No nome da UO, digite **`TestCWEOU`** e escolha Create organizational unit (Criar unidade organizacional).

Para ver a entrada de log do EventBridge

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Na página de navegação, escolha Logs.
3. Na página Log Groups (Registrar grupos), escolha o grupo associado à sua função do Lambda: /aws/lambda/LogOrganizationEvents.
4. Cada grupo contém um ou mais streams e deve haver um grupo para hoje. Escolha-o.

5. Visualize o log. Você deve ver linhas semelhantes às seguintes:




6. Selecione a linha do meio da entrada para ver o texto JSON completo do evento recebido. Você pode ver todos os detalhes da solicitação da API nas partes `requestParameters` e `responseElements` da saída:

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
```

```
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```

7. Verifique se existe em sua conta de e-mail uma mensagem de OrgsCWEvnt (o nome de exibição do seu tópico do Amazon SNS). O corpo do e-mail contém a mesma saída de texto JSON que a entrada de log mostrada na etapa anterior.

## Limpar: remover os recursos que não são mais necessários

Para evitar ser cobrado, você deve excluir qualquer recurso AWS que criou como parte deste tutorial que você não deseja manter.

Para limpar o seu ambiente AWS

1. Use o console do CloudTrail para excluir a trilha chamada **`My-Test-Trail`** que você criou na etapa 1.
2. Se você criou um bucket do Amazon S3 na etapa 1, use o console do Amazon S3 para excluí-lo.
3. Use o console do Lambda para excluir a função chamada **`LogOrganizationEvents`** que você criou na etapa 2.
4. Use o console do Amazon SNS para excluir o tópico do Amazon SNS chamado **`OrganizationsCloudWatchTopic`** que você criou na etapa 3.
5. Use o console do CloudWatch para excluir a regra do EventBridge chamada **`OrgsMonitorRule`** que foi criada na etapa 4.
6. Use o console do Organizations para excluir a UO denominada **`TestCWEOU`** que você criou na etapa 5.

Isso é tudo. Neste tutorial, você configurou o EventBridge para monitorar alterações em sua organização. Você configurou uma regra que é acionada quando os usuários invocam operações específicas do AWS Organizations. A regra executou uma função do Lambda que registrou o evento no log e enviou um e-mail com detalhes sobre o evento.

# Práticas recomendadas o gerenciamento de várias contas

Siga estas recomendações para obter ajuda para configurar e gerenciar um ambiente com várias contas no AWS Organizations.

Tópicos



## Gerenciar suas contas em uma única organização

Recomendamos criar uma única organização e gerenciar todas as suas contas nessa organização. Uma organização é um limite de segurança que permite manter a consistência entre contas em seu ambiente. Você pode aplicar centralmente políticas ou configurações de nível de serviço em todas as contas de uma organização. Se você deseja habilitar políticas consistentes, visibilidade central e controles programáticos em seu ambiente de várias contas, a melhor forma de fazer isso é com uma única organização.

# Usar uma senha forte para o usuário raiz

Recomendamos utilizar uma senha forte e exclusiva. Diversos gerenciadores de senhas e algoritmos e ferramentas de geração de senhas fortes podem ajudar você a alcançar esses objetivos. Para obter mais informações, consulte Alterar a senha para o Usuário raiz da conta da AWS. Use a política de segurança de informações da sua empresa para gerenciar o armazenamento a longo prazo e o acesso à senha do usuário raiz. Recomendamos armazenar a senha em um sistema gerenciador de senhas ou equivalente que atenda aos requisitos de segurança da sua organização. Para evitar criar uma dependência circular, não armazene a senha do usuário-raiz com ferramentas que dependam de serviços da AWS em que faz login com a conta protegida. Seja qual for o método escolhido, recomendamos priorizar a resiliência e considerar potencialmente exigir que vários atores autorizem o acesso a este cofre para proporcionar proteção aprimorada. Qualquer acesso à senha ou a seu local de armazenamento deve ser registrado e monitorado. Para obter mais recomendações de senha do usuário raiz, consulte As práticas recomendadas do usuário raiz para a Conta da AWS.

# Documentar os processos quanto ao uso das credenciais do usuário raiz

Documente a execução de processos importantes à medida eles são realizados para garantir a existência de um registro dos indivíduos envolvidos em cada etapa. Para gerenciar a senha, recomendamos utilizar um gerenciador de senhas criptografadas seguro. Também é importante fornecer documentação sobre quaisquer exceções e eventos imprevistos que possam ocorrer. Para obter mais informações, consulte Solução de problemasAWS Management Console de login no AWSGuia do usuário de login e Tarefas que exigem credenciais de usuário root no Guia do usuário do IAM.

Teste e valide se você continua a ter acesso ao usuário raiz e se o número de telefone celular está operacional pelo menos uma vez a cada trimestre. Isso ajuda a garantir à empresa que o processo funciona e que você pode manter o acesso ao usuário raiz. Além disso, demonstra que as pessoas responsáveis pelo acesso de usuário raiz entendem as etapas que devem ser executadas para que o processo seja bem-sucedido. Para reduzir o tempo de resposta e aumentar a taxa de sucesso, é importante garantir que todos os profissionais envolvidos em um processo entendam exatamente o que devem fazer em caso de necessidade de acesso.

# Habilitar a MFA para as credenciais do usuário raiz

Recomendamos habilitar vários dispositivos de autenticação multifator (MFA) para o usuário raiz da Conta da AWS e usuários do IAM em suas Contas da AWS. Isso permite aumentar o nível de segurança em suas Contas da AWS e simplificar o gerenciamento do acesso a usuários altamente privilegiados, como o usuário raiz da Conta da AWS. Para atender às diferentes necessidades do cliente, a AWS oferece suporte a três tipos de dispositivos de MFA para IAM, incluindo chaves de segurança FIDO, aplicações autenticadoras virtuais e tokens de hardware com senha de uso único com marcação temporal (TOTP).

Cada tipo de autenticador tem propriedades físicas e de segurança ligeiramente diferentes que são mais adequadas para diferentes casos de uso. As chaves de segurança FIDO2 oferecem o mais alto nível de garantia e são resistentes a phishing. Qualquer forma de MFA oferece uma postura de segurança mais robusta do que a autenticação somente por senha, e é altamente recomendável adicionar alguma forma de MFA à sua conta. Selecione o tipo de dispositivo que melhor se alinha aos seus requisitos operacionais e de segurança.

Se você escolher um dispositivo alimentado por bateria para seu autenticador principal, como um token de hardware com TOTP, considere também registrar um autenticador que não dependa de bateria como mecanismo de backup. Verificar regularmente a funcionalidade do dispositivo e substituí-lo antes da data de validade também é essencial para manter o acesso ininterrupto. Independentemente do tipo de dispositivo escolhido, recomendamos registrar pelo menos dois dispositivos (o IAM oferece suporte a até oito dispositivos MFA por usuário) para aumentar sua resiliência contra perda ou falha do dispositivo.

Siga a política de segurança da informação da sua organização para o armazenamento do dispositivo MFA. Recomendamos armazenar o dispositivo MFA separadamente da senha associada. Isso garante que o acesso à senha e ao dispositivo de MFA exija recursos diferentes (pessoas, dados e ferramentas). Essa separação adiciona uma camada extra de proteção contra acesso não autorizado. Também recomendamos que registrar e monitorar qualquer acesso ao dispositivo MFA ou seu local de armazenamento. Isso ajuda a detectar e responder a qualquer acesso não autorizado.

Para obter mais informações, consulte Proteja o acesso do seu usuário raiz com autenticação multifator (MFA) no Guia do usuário do IAM. Para obter instruções sobre como habilitar a MFA, consulte Usar a autenticação multifator (MFA) na AWS e Habilitar dispositivos MFA para usuários na AWS.

# Aplique controles para monitorar o acesso às credenciais do usuário-raiz

O acesso às credenciais do usuário-raiz deve ser um evento raro. Crie alertas usando ferramentas como o Amazon EventBridge para anunciar o login e o uso das credenciais do usuário raiz da conta de gerenciamento. Este alerta deve incluir, entre outras informações, o endereço de e-mail usado para o próprio usuário raiz. Esse alerta deve ser significativo e difícil de não ser visto. Para ver um exemplo, consulte Monitorar e notificar atividade de usuário-raiz da Conta da AWS. Verifique se os profissionais que receberão um alerta são capazes de entender como validar que o acesso do usuário raiz é esperado e se eles sabem como escalar a situação se acreditarem que um incidente de segurança está em andamento. Para obter mais informações, consulte Denunciar e-mails suspeitos ou Relatórios de vulnerabilidades. Como alternativa, você pode Entrar em contato com a AWS para obter assistência e orientação adicional.

# Mantenha o número de telefone de contato atualizado

Para recuperar o acesso à sua Conta da AWS, é crucial ter um número de telefone de contato válido e ativo que permita receber mensagens de texto ou chamadas. Recomendamos usar um número de telefone dedicado para garantir que a AWS possa entrar em contato com você para fins de suporte e recuperação da conta. Você pode visualizar e gerenciar facilmente os números de telefone da sua conta via AWS Management Console ou por meio das APIs de gerenciamento de contas.

Existem várias maneiras de obter um número de telefone dedicado que garanta que a AWS possa entrar em contato com você. É altamente recomendável obter um cartão SIM dedicado e um telefone físico. Armazene o telefone e o SIM em segurança a longo prazo para garantir que o número de telefone permaneça sempre disponível para recuperação da conta. Certifique-se também de que a equipe responsável pela conta de telefonia celular entenda a importância desse número, mesmo que ele permaneça inativo por longos períodos. É essencial manter esse número de telefone confidencial em sua organização para garantir proteção adicional.

Documente o número de telefone na página do console de Informações de contato da AWS e compartilhe seus detalhes com as equipes específicas em sua organização que precisam conhecê-lo. Essa abordagem ajuda a minimizar o risco associado à transferência do número de telefone para um SIM diferente. Armazene o telefone de acordo com sua política de segurança de informações existente. Porém, não armazene o telefone no mesmo local que as outras informações de credenciais relacionadas. Qualquer acesso ao telefone ou a seu local de armazenamento deve

ser registrado e monitorado. Se o número de telefone associado a uma conta mudar, implemente processos para atualizar o número de telefone em sua documentação existente.

## Usar um endereço de e-mail de grupo contas raiz

Use um endereço de e-mail gerenciado pela sua empresa. Use um endereço de e-mail que encaminhe as mensagens recebidas diretamente para um grupo de usuários. Caso a AWS precise entrar em contato com o proprietário da conta, por exemplo, para confirmar o acesso, a mensagem de e-mail será distribuída para várias partes. Essa abordagem ajuda a reduzir o risco de atrasos na resposta, mesmo que as pessoas estejam de férias, estejam doentes ou deixem a empresa.

## Agrupar workloads com base na finalidade comercial e não na estrutura hierárquica

Recomendamos isolar os ambientes e dados de workloads de produção em suas OUs de nível superior orientadas a workloads. Suas OUs devem se basear em um conjunto comum de controles, em vez de espelhar a estrutura hierárquica da empresa. Além das OUs de produção, recomendamos definir uma ou mais OUs de não produção que contenham contas e ambientes de workload usados para desenvolver e testar workloads. Para obter orientação adicional, consulte Organizar OUs orientadas a workloads.

## Use várias contas para organizar suas workloads

Uma Conta da AWS fornece segurança natural, acesso e limites de cobrança para seus recursos da AWS. Usar várias contas oferece algumas vantagens, pois permite distribuir cotas em nível de conta e limites de taxa de solicitação de API, além de benefícios adicionais listados aqui. Recomendamos usar contas básicas organizacionais diferentes, como contas para segurança, log e infraestrutura. Para contas de workload, é necessário separar as workloads de produção das workloads de teste/desenvolvimento em contas diferentes.

## Habilite serviços da AWS no nível organizacional usando o console de serviço ou operações de API/CLI

Como prática recomendada, sugerimos habilitar ou desabilitar todos os serviços aos quais você gostaria de integrar ao AWS Organizations usando o console desse serviço ou os equivalentes de comando da CLI e operações de API/CLI. Com esse método, o serviço da AWS pode executar todas

as etapas de inicialização necessárias para sua organização, como criar recursos necessários e limpar os recursos ao desabilitar o serviço. O AWS Account Management é o único serviço que requer o uso do console ou das APIs do AWS Organizations para ser habilitado. Para revisar a lista de serviços integrados ao AWS Organizations, consulte AWS serviços que você pode usar com AWS Organizations.

## Usar ferramentas de faturamento para monitorar custos e otimizar o uso de recursos

Ao gerenciar uma organização, você recebe uma fatura consolidada que cobre todas as cobranças das contas em sua organização. Para usuários corporativos que precisam de acesso à visibilidade dos custos, é possível fornecer um perfil na conta de gerenciamento com permissões restritas de somente leitura para revisar as ferramentas de faturamento e custo. Por exemplo, você pode criar um conjunto de permissões que forneça acesso aos relatórios de faturamento ou usar o AWS Cost Explorer Service (uma ferramenta para visualizar tendências de custo ao longo do tempo) e serviços economicamente eficientes, como o Amazon S3 Storage Lens e AWS Compute Optimizer.

## Planeje a estratégia de marcação e a aplicação de tags em todos os recursos da sua organização

À medida que suas contas e workloads aumentam, as tags podem ser um recurso útil para controlar os custos, o controle de acesso e a organização de recursos. Para estratégias de nomenclatura de tags, siga as orientações em Como marcar seus recursos da AWS. Além dos recursos, você pode criar tags na raiz e nas contas, OUs e políticas da organização. Consulte Criar sua estratégia de tags para obter informações adicionais.

## Práticas recomendadas para a conta de gerenciamento

Siga estas recomendações para ajudar a proteger a segurança da conta de gerenciamento no AWS Organizations. Essas recomendações pressupõem que você também siga as práticas recomendadas de uso do usuário-raiz somente para as tarefas que realmente o exigem.

Tópicos

- Limitar quem tem acesso à conta de gerenciamento
- Revisar e controlar quem tem acesso

- Use a conta de gerenciamento somente para tarefas que exijam a conta de gerenciamento
- Evite implantar workloads na conta de gerenciamento da organização
- Delegar responsabilidades fora da conta de gerenciamento para descentralização

## Limitar quem tem acesso à conta de gerenciamento

A conta de gerenciamento é essencial para todas as tarefas administrativas mencionadas, como gerenciamento de contas, políticas, integração com outros serviços da AWS, faturamento consolidado e assim por diante. Portanto, você deve restringir e limitar o acesso à conta de gerenciamento somente para os usuários administradores que precisam de direitos para fazer alterações na organização.

## Revisar e controlar quem tem acesso

Para garantir a manutenção do acesso à conta de gerenciamento, revise periodicamente quem em sua empresa tem acesso ao endereço de e-mail, senha, MFA e número de telefone associados a ela. Alinhe sua revisão com os procedimentos existentes da empresa. Adicione uma revisão mensal ou trimestral dessas informações para verificar se apenas as pessoas corretas têm acesso. Certifique-se de que o processo para recuperar ou redefinir o acesso às credenciais do usuário-raiz não dependa de nenhum indivíduo específico para ser concluído. Todos os processos devem levar em conta a possibilidade de pessoas estarem indisponíveis.

## Use a conta de gerenciamento somente para tarefas que exijam a conta de gerenciamento

Recomendamos usar a conta de gerenciamento e seus usuários e perfis somente para as tarefas que só podem ser executadas por essa conta. Armazene todos os seus recursos da AWS em outras Contas da AWS da organização e mantenha-os fora da conta de gerenciamento. Um motivo importante para manter seus recursos em outras contas é porque as políticas de controle de serviço (SCPs) do Organizations não funcionam para restringir os usuários ou as funções na conta de gerenciamento. Separar seus recursos da conta de gerenciamento também ajuda a entender os lançamentos em suas faturas.

## Evite implantar workloads na conta de gerenciamento da organização

As operações privilegiadas podem ser executadas na conta de gerenciamento de uma organização, e os SCPs não se aplicam à conta de gerenciamento. É por isso que você deve limitar os recursos e

dados da nuvem contidos na conta de gerenciamento somente àqueles que devem ser gerenciados nessa conta.

## Delegar responsabilidades fora da conta de gerenciamento para descentralização

Sempre que possível, recomendamos delegar responsabilidades e serviços fora da conta de gerenciamento. Forneça às suas equipes permissões em suas próprias contas para gerenciar as necessidades da organização para que não seja necessário acessar a conta de gerenciamento. Além disso, é possível registrar vários administradores delegados para serviços que oferecem suporte a essa funcionalidade, como o AWS Service Catalog para compartilhar software em toda a organização ou o AWS CloudFormation StackSets para criar e implantar pilhas.

Para obter mais informações, consulte Arquitetura de referência de segurança, Organizar seu ambiente da AWS usando várias contas e AWS serviços que você pode usar com AWS Organizations para obter sugestões de como registrar contas-membro como administrador delegado para vários serviços da AWS. Para obter mais informações sobre como configurar administradores delegados, consulte Habilitar uma conta de administrador delegado para o AWS Account Management e Administrador delegado para AWS Organizations.

# Práticas recomendadas para contas-membro

Siga estas recomendações para ajudar a proteger a segurança das contas membro em sua organização. Essas recomendações pressupõem que você também siga as práticas recomendadas de uso do usuário-raiz somente para as tarefas que realmente o exigem.

Tópicos

- Definir o nome e os atributos da conta
- Escalar com eficiência o ambiente e o uso da conta
- Use um SCP para restringir o que o usuário-raiz de suas contas-membro pode fazer

## Definir o nome e os atributos da conta

Para suas contas-membro, use uma estrutura de nomes e um endereço de e-mail que reflita o uso da conta. Por exemplo, `Workloads+fooA+dev@domain.com` para `WorkloadsFooADev`, `Workloads+fooB+dev@domain.com` para `WorkloadsFooBDev`. Se houver tags personalizadas

definidas para sua organização, recomendamos a você atribuir essas tags em contas que reflitam o uso da conta, o centro de custos, o ambiente e o projeto. Isso torna mais fácil identificar, organizar e pesquisar contas.

## Escalar com eficiência o ambiente e o uso da conta

Ao escalar, antes de criar novas contas, certifique-se de que ainda não existam contas para necessidades semelhantes para evitar duplicações desnecessárias. As Contas da AWS devem se basear em requisitos de acesso comuns. Se você planeja reutilizar as contas, como uma conta de sandbox ou equivalente, recomendamos  limpar quaisquer recursos ou workloads desnecessários das contas, mas salve as contas para uso futuro.

Antes de encerrar contas, observe que elas estão sujeitas aos limites de cota de fechamento de contas. Para obter mais informações, consulte Cotas para AWS Organizations. Considere implementar um processo de limpeza para reutilizar contas em vez de encerrá-las e criar novas quando possível. Dessa forma, você evitará incorrer em custos com a execução de recursos e atingir os limites da API CloseAccount.

## Use um SCP para restringir o que o usuário-raiz de suas contas-membro pode fazer

Recomendamos que você crie uma política de controle de serviço (SCP) na organização e anexe-a à raiz da organização para que ela se aplique a todas as contas-membro. Para obter mais informações, consulte Proteja as credenciais de usuário raiz da conta Organizations.

Você pode negar todas as ações da raiz, exceto uma ação exclusiva à raiz que deve ser executada em sua conta-membro. Por exemplo, a SCP a seguir impede que o usuário raiz em qualquer conta-membro faça qualquer chamada de API de serviço da AWS, exceto “Atualizar uma política de bucket do S3 que foi configurada incorretamente e nega acesso a todas as entidades principais” (uma das ações que exigem credenciais de raiz). Para obter mais informações, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

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

    "Statement": [

        {
```

```
            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
"StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }

       }

   ]
}
```

Na maioria das circunstâncias, quaisquer tarefas administrativas podem ser executadas por um perfil do AWS Identity and Access Management (IAM) na conta-membro com as permissões de administrador relevantes. Esses perfis devem ter controles adequados aplicados para limitar, registrar e monitorar atividades.

# Criar e gerenciar uma organização

Você pode executar as seguintes tarefas usando a console do AWS Organizations ou executando um comando do AWS Command Line Interface (AWS CLI) ou as operações equivalentes da API do AWS SDK:

- Criar uma organização. Crie sua organização com a sua conta atual como conta de gerenciamento. Crie contas-membro em sua organização e convide outras contas para se unir à sua organização.
- Ativar todos os recursos em sua organização. A habilitação de todos os recursos é a forma preferida de trabalhar com o AWS Organizations. Quando você cria uma organização, você tem a opção de habilitar todos os recursos ou um subconjunto de recursos para consolidar o faturamento. A habilitação de todos os recursos é o padrão, e inclui recursos de faturamento consolidado.

  Com todos os recursos habilitados, você pode usar os recursos avançados disponíveis no gerenciamento de contas no AWS Organizations, como políticas de controle de serviço (SCPs). As SCPs oferecem controle central sobre o máximo disponível permissões para todas as contas de sua organização, ajudando você a manter suas contas dentro diretrizes de controle de acesso de sua organização.
- Visualizar detalhes sobre sua organização. Visualize detalhes sobre sua organização e as raízes, unidades organizacionais (UOs) e contas correspondentes.
- Excluir uma organização. Exclua uma organização quando ela não for mais necessária.

> **Note**
>
> Os procedimentos nesta seção especificam as permissões mínimas necessárias para executar as tarefas. Eles normalmente se aplicam à API ou ao acesso à ferramenta de linha de comando.
> A execução de uma tarefa no console pode exigir permissões adicionais. Por exemplo, você pode conceder permissões somente leitura a todos os usuários de sua organização e conceder outras permissões que permitem que usuários selecionados executem tarefas específicas.

# Criar uma organização

Você pode criar uma organização que começa com sua Conta da AWS como a conta de gerenciamento. Ao criar uma organização, você pode escolher se a organização oferece suporte a todos os recursos (recomendado) ou somente a recursos de faturamento consolidado.

Depois de criar uma organização, você pode adicionar contas à sua organização desses modos a partir da conta de gerenciamento:

- Criar outras Contas da AWS que são adicionadas automaticamente à sua organização como contas-membro
- Depois de verificar o seu endereço de e-mail, convide Contas da AWS existentes para participar da sua organização como contas-membro

## Criar uma organização

É possível criar uma organização usando o AWS Management Console ou usando um comando da AWS CLI ou uma das APIs do SDK.

> **Permissões mínimas**
>
> Para criar uma organização com sua Conta da AWS atual, você deve ter as seguintes permissões:
>
> - `organizations:CreateOrganization`
> - `iam:CreateServiceLinkedRole`
>
> Você pode restringir essa permissão apenas para o principal do serviço `organizations.amazonaws.com`.

AWS Management Console

Para criar uma organização do

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

2. Por padrão, a organização é criada com todos os recursos habilitados. No entanto, é possível escolher uma das seguintes etapas:

   - Para criar uma organização com todos os recursos habilitados, na página de introdução, escolha Create an organization (Criar uma organização).
   - Para criar uma organização apenas com recursos de Faturamento consolidado, na página de introdução e em Create an organization (Criar uma organização), escolha consolidated billing features (recursos de faturamento consolidado) e, na caixa de diálogo de confirmação, escolha Create an organization (Criar uma organização).

   Se acidentalmente escolher a opção errada, você pode ir imediatamente para a página Settings (Configurações) e escolher Delete organization (Excluir organização) e começar de novo.

3. A organização é criada e a página Contas da AWS é exibida. A única conta presente é sua conta de gerenciamento, e ela está atualmente armazenada na unidade organizacional-raiz (UO).

   Se necessário, o Organizations envia um e-mail de verificação automaticamente para o endereço associado à sua conta de gerenciamento. Talvez haja um atraso até você receber o e-mail de verificação. Verifique o endereço de e-mail em 24 horas. Para mais informações, consulte Verificação do endereço de e-mail. Você pode criar contas novas para aumentar sua organização sem verificar o endereço de e-mail de sua conta de gerenciamento. Entretanto, para convidar contas existentes, você deve primeiro fazer a verificação de e-mail.

   > **Note**
   >
   > Se essa conta já confirmou seu endereço de e-mail anteriormente, isso não acontecerá novamente quando você usar a conta para criar uma organização.

AWS CLI & AWS SDKs

Para criar uma organização do

Você pode usar um dos seguintes comandos para criar uma organização:

- AWS CLI: create-organization

O exemplo a seguir cria uma organização e torna a Conta da AWS atualmente conectada a conta de gerenciamento da organização.

```
$ aws organizations create-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [  ...DEPRECATED - DO NOT USE ... ]
    }
}
```

> **Important**
>
> O campo `AvailablePolicyTypes` está defasado e não contém informações precisas sobre as políticas habilitadas na sua organização. Para ver a lista precisa e completa dos tipos de política que estão realmente habilitados para a organização, use o comando `ListRoots`, como descrito na parte sobre a AWS CLI da seguinte seção.

- AWS SDKs: CreateOrganization

Agora é possível adicionar contas à sua organização da seguinte forma:

- Para criar uma Conta da AWS que automaticamente faça parte de sua organização da AWS, consulte Criar uma conta-membro na sua organização.
- Para convidar uma conta existente à sua organização, consulte Convidar um homem Conta da AWS para se juntar à sua organização.

## Verificação do endereço de e-mail

Depois de criar uma organização e para convidar contas a participar, você deverá confirmar que é proprietário do endereço de e-mail fornecido para a conta de gerenciamento da organização.

Quando você cria uma organização, se a conta de gerenciamento não tiver sido verificada anteriormente, a AWS envia automaticamente um e-mail de verificação para o endereço de e-mail especificado. Talvez haja um atraso até você receber o e-mail de verificação.

Em 24 horas, siga as instruções no e-mail para verificar o seu endereço de e-mail.

Se não verificar o seu endereço de e-mail em até 24 horas, você poderá reenviar a solicitação de verificação. Dessa maneira, você pode convidar outras Contas da AWS para a sua organização. Se você não receber o e-mail de verificação, verifique se o seu endereço de e-mail está correto e, se necessário, modifique-o.

- Para descobrir o endereço de e-mail associado à sua conta de gerenciamento, consulte Visualização de detalhes de uma organização na conta de gerenciamento.
- Para alterar o endereço de e-mail associado à sua conta de gerenciamento, consulte Gerenciar uma Conta da AWS no Manual do usuário do AWS Billing.

AWS Management Console

Para reenviar a solicitação de verificação

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Navegue até a página Settings (Configurações) e escolha Send verification request (Enviar solicitação de verificação). A opção só estará presente se a conta de gerenciamento não tiver sido verificada.
3. Verifique o endereço de e-mail em 24 horas.

   Depois de verificar o seu endereço de e-mail, você poderá convidar outras Contas da AWS para a sua organização. Para mais informações, consulte Convidar um homem Conta da AWS para se juntar à sua organização.

Se você alterar o endereço de e-mail da conta de gerenciamento, o status da conta será revertido para "e-mail não verificado", e você deverá concluir o processo de verificação de seu novo endereço de e-mail.

> **Note**
>
> Se você convidou contas para ingressar em sua organização antes de alterar o endereço de e-mail da conta de gerenciamento e esses convites ainda não foram aceitos, eles não poderão ser aceitos até que você verifique o novo endereço de e-mail da conta de gerenciamento. Use o procedimento anterior para reenviar a solicitação de verificação. Depois de concluir o processo respondendo ao e-mail, suas contas convidadas poderão aceitar os convites.

# Habilitar todos os recursos na organização

O AWS Organizations tem dois conjuntos de recursos disponíveis:

- Todos os recursos – Este conjunto de recursos é a forma preferida de trabalhar com o AWS Organizations, e inclui recursos de faturamento consolidado. Quando você cria uma organização, a habilitação de todos os recursos é o padrão. Com todos os recursos habilitados, você pode usar os recursos avançados disponíveis no gerenciamento de contas no AWS Organizations, tais como integração com os serviços compatíveis da AWS e políticas de gerenciamento da organização.
- Recursos de faturamento consolidado – Todas as organizações suportam este subconjunto de recursos de faturamento consolidado, que fornece ferramentas de gerenciamento básicas que você pode usar para gerenciar centralmente as contas de sua organização.

Se você criar uma organização apenas com os recursos de faturamento consolidado, poderá habilitar todos os recursos posteriormente. Esta página descreve o processo de habilitação de todos os recursos.

## Antes de habilitar todos os recursos

Antes de mudar de uma organização que oferece suporte apenas a recursos de faturamento consolidado para uma organização que oferece suporte a todos os recursos, observe o seguinte:

- Quando você inicia o processo para habilitar todos os recursos, o AWS Organizations envia uma solicitação para cada conta-membro convidada para ingressar em sua organização. Cada conta convidada deve aprovar a ativação de todos os recursos aceitando a solicitação. Somente então você poderá concluir o processo para ativar todos os recursos em sua organização. Se uma conta recusar a solicitação, você deve remover a conta de sua organização ou reenviar a solicitação. A

solicitação deve ser aceita antes que você possa concluir o processo de habilitação de todos os recursos. As contas que você criou usando o AWS Organizations não recebem uma solicitação porque não precisam aprovar o controle adicional.

- Você pode continuar convidando contas para sua organização enquanto habilita todos os recursos. O proprietário de uma conta convidada é informado pelo convite se ele está ingressando em uma organização apenas com faturamento consolidado ou com todos os recursos habilitados.
  - Se você convidar uma conta durante o processo para habilitar todos os recursos, o convite indica que a organização em que a conta está ingressando tem todos os recursos habilitados. Se você cancelar o processo para habilitar todos os recursos antes que a conta aceite o convite, esse convite será cancelado. Você deve convidar a conta novamente para ser membro de uma organização apenas com os recursos de faturamento consolidado.
  - Se você convidar uma conta e o convite não tiver sido aceito antes de você iniciar o processo para habilitar todos os recursos, esse convite é cancelado, porque o convite indica que a organização tem recursos de faturamento consolidados apenas. Você deve convidar a conta novamente para ser membro de uma organização com todos os recursos habilitados.
- Você também pode continuar criando contas na organização. Esse processo não é afetado por essa alteração.
- O AWS Organizations verifica que toda conta-membro tenha uma função vinculada ao serviço chamada `AWSServiceRoleForOrganizations`. Essa função é obrigatória em todas as contas para ativar todos os recursos. Se você excluiu a função em uma conta de convidado, aceitar o convite para ativar todos os recursos recria a função. Se você excluiu a função em uma conta que foi criada usando AWS Organizations, essa conta recebe um convite especificamente para recriar essa função. Todos esses convites devem ser aceitos para a organização concluir o processo de habilitação de todos os recursos.
- Como a habilitação de todos os recursos possibilita o uso de SCPs, certifique-se de que os administradores de sua conta compreendem os efeitos da anexação de SCPs à organização, às unidades organizacionais ou às contas. Uma SCP pode restringir o que os usuários e até mesmo os administradores podem fazer nas contas afetadas. Por exemplo, a conta de gerenciamento pode aplicar SCPs que podem impedir que contas-membro saiam da organização.
- A conta de gerenciamento não é afetada por nenhuma SCP. Você não pode limitar o que os usuários e as funções na conta de gerenciamento podem fazer aplicando SCPs. As SCPs afetam somente contas-membro.
- A migração de recursos de faturamento consolidado para todos os recursos é unidirecional. Você não pode mudar uma organização com todos os recursos habilitados de volta para apenas recursos de faturamento consolidado.

- (Não recomendado) Se sua organização tiver apenas recursos de faturamento consolidado habilitados, os administradores da conta-membro podem optar por excluir a função vinculada ao serviço chamada `AWSServiceRoleForOrganizations`. No entanto, quando você habilita todos os recursos em uma organização, essa função é necessária e é recriada em todas as contas como parte da aceitação do convite para habilitar todos os recursos. Para obter mais informações sobre como o AWS Organizations usa esta função, consulte AWS Organizations e funções vinculadas ao serviço.

## Iniciar processo para habilitar todos os recursos

Quando faz login com permissões na conta de gerenciamento de sua organização, pode iniciar o processo para habilitar todos os recursos. Para fazer isso, conclua as seguintes etapas.

> **Permissões mínimas**
>
> Para ativar todos os recursos em sua organização, você deve ter as seguintes permissões:
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations

AWS Management Console

Para pedir para as contas-membro convidadas aceitarem a ativação de todos os recursos na organização

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Settings (Configurações), escolha Begin process to enable all features (Iniciar processo para ativar todos os recursos).
3. Na página Enable all features (Ativar todos os recursos), confirme que entendeu que não é possível retornar para recursos de faturamento consolidado apenas depois que você alternar escolhendo Begin process to enable all features (Iniciar processo para ativar todos os recursos).

O AWS Organizations envia uma solicitação para cada conta convidada (não criada) na organização solicitando a aprovação para ativar todos os recursos na organização. Se você tiver contas que foram criadas usando o AWS Organizations e o administrador da conta-membro tiver excluído a função vinculada ao serviço chamada `AWSServiceRoleForOrganizations`, o AWS Organizations enviará àquela conta uma solicitação para recriar a função.

O console exibe a lista Request approval status (Solicitar status de aprovação) para as contas convidadas.

> **Tip**
>
> Para voltar a esta página mais tarde, abra a página Settings (Configurações) e, na seção Request sent date (Data de envio do pedido), escolha View status (Visualizar status).

4. A página Enable all features (habilitar todos os recursos mostra o status atual da solicitação para cada conta na organização. As contas que aceitaram a solicitação mostram um status de ACCEPTED (ACEITO). As contas que ainda não concordaram mostram um status de OPEN (ABERTO).

AWS CLI & AWS SDKs

Para pedir para as contas-membro convidadas aceitarem a ativação de todos os recursos na organização

Você pode usar um dos seguintes comandos para habilitar todos os recursos em uma organização:

- AWS CLI: enable-all-features

  O comando a seguir inicia o processo para habilitar todos os recursos na organização.

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
```

```
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

A saída mostra os detalhes do handshake com o qual as contas dos membros convidados devem concordar.

- AWS SDKs: EnableAllFeatures

Observações

- Uma contagem regressiva de 90 dias começa quando a solicitação é enviada para as contas-membro. Todas as contas devem aprovar a solicitação dentro desse período. Caso contrário, a solicitação expirará. Se a validade da solicitação expirar, todas as solicitações relacionadas a essa tentativa são canceladas, e você precisa recomeçar na etapa 2.
- Após a solicitação para ativar todos os recursos ser feita, todos os convites de conta não aceitos existentes serão cancelados.
- Durante o processo de migração de todos os recursos, ainda será possível iniciar novos convites para contas e criar novas contas.

Depois que todas as contas da organização aprovarem as solicitações, você poderá finalizar o processo e habilitar todos os recursos. Você também pode finalizar o processo imediatamente caso

sua organização não tenha nenhuma conta-membro convidada. Para finalizar o processo, continue com Finalizar o processo para habilitar todos os recursos.

## Aprovar solicitação para habilitar todos os recursos ou recriar a função vinculada ao serviço

Quando faz login em uma das contas-membro convidadas da organização, você pode aprovar uma solicitação na conta de gerenciamento. Se sua conta foi originalmente convidada a ingressar na organização, o convite será para ativar todos os recursos e implicitamente incluir a aprovação para recriar a função `AWSServiceRoleForOrganizations`, se necessário. Se a sua conta tiver sido criada usando o AWS Organizations e você excluiu a função vinculada ao serviço `AWSServiceRoleForOrganizations`, receberá um convite apenas para recriar a função. Para fazer isso, conclua as seguintes etapas.

**Important**

Se você habilitar todos os recursos, a conta de gerenciamento da organização poderá aplicar controles baseados em políticas na sua conta-membro. Esses controles podem restringir o que os usuários e até mesmo o que você, como administrador, poderá fazer na conta. Essas restrições podem impedir que sua conta saia da organização.

**Permissões mínimas**

Para aprovar uma solicitação para ativar todos os recursos para a sua conta membro, você deverá ter as seguintes permissões:

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations
- `organizations:ListHandshakesForAccount` – necessário somente ao usar o console do Organizations
- `iam:CreateServiceLinkedRole` – necessário somente se for preciso recriar a função `AWSServiceRoleForOrganizations` na conta membro

AWS Management Console

Para aceitar a solicitação de ativação de todos os recursos na organização

1. Faça login no console do AWS Organizations no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta-membro.
2. Leia o que significa a aceitação da solicitação para todos os recursos na organização para a sua conta e escolha Aceitar. A página continua mostrando o processo como incompleto até que todas as contas na organização aceitem as solicitações e o administrador da conta de gerenciamento finalize o processo.

AWS CLI & AWS SDKs

Para aceitar a solicitação de ativação de todos os recursos na organização

Para aceitar a solicitação, você deve aceitar o handshake com `"Action": "APPROVE_ALL_FEATURES"`.

- AWS CLI:
  - accept-handshake
  - list-handshakes-for-account

  O exemplo a seguir mostra como listar os handshakes disponíveis para sua conta. O valor de `"Id"` na quarta linha da saída é o valor que você precisa para o próximo comando.

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
```

```
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
}
```

O exemplo a seguir usa o ID do handshake do comando anterior para aceitar esse handshake.

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
```

```
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
}
```

- AWS SDKs:
  - list-handshakes-for-account
  - AcceptHandshake

## Finalizar o processo para habilitar todos os recursos

Todas as contas-membro convidadas devem aprovar a solicitação para habilitar todos os recursos. Se não houver contas membros convidadas na organização, a página Progresso de ativação de todos os recursos indicará com um banner verde que você pode finalizar o processo.

> **Permissões mínimas**
>
> Para finalizar o processo de ativação de todos os recursos para a organização, você deve ter as seguintes permissões:
>
> - `organizations:AcceptHandshake`
> - `organizations:ListHandshakesForOrganization`

- `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations

### AWS Management Console

Para finalizar o processo para ativar todos os recursos

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Settings (Configurações), se todas as contas convidadas aceitarem a solicitação para habilitar todos os recursos, uma caixa verde aparecerá na parte superior da página para informar você. Na caixa verde, escolha Go to finalize (Ir para finalizar).
3. Na página Enable all features (Habilitar todos os recursos), escolha Finalize (Finalizar) e, na caixa de diálogo de confirmação, escolha Finalize (Finalizar) novamente.
4. A organização agora tem todos os recursos ativados.

### AWS CLI & AWS SDKs

Para finalizar o processo para ativar todos os recursos

Para finalizar o processo, você deve aceitar o handshake com `"Action": "ENABLE_ALL_FEATURES"`.

- AWS CLI:
  - list-handshakes-for-organization
  - accept-handshake

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
```

```
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

O exemplo a seguir mostra como listar os handshakes disponíveis para a organização. O valor de `"Id"` na quarta linha da saída é o valor que você precisa para o próximo comando.

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
```

```
    }
}
```

- AWS SDKs:
  - AcceptHandshake
  - AcceptHandshake

Os próximos passos:

- Habilite os tipos de políticas que você deseja usar. Depois disso, você pode anexar políticas para administrar as contas em sua organização. Para obter mais informações, consulte Gerenciando políticas em AWS Organizations.
- Habilite a integração com os serviços compatíveis. Para obter mais informações, consulte Usar o AWS Organizations com outros serviços da AWS.

# Visualizar detalhes sobre a organização

Você pode executar as seguintes tarefas para visualizar detalhes sobre elementos de sua organização.

Tópicos

- Visualização de detalhes de uma organização na conta de gerenciamento
- Visualizar os detalhes do contêiner raiz
- Visualização de detalhes de uma UO
- Visualizar detalhes de uma conta
- Visualizar detalhes de uma política

## Visualização de detalhes de uma organização na conta de gerenciamento

Quando faz login na conta de gerenciamento da organização no console do AWS Organizations, você pode visualizar os detalhes da organização.

> **Permissões mínimas**
>
> Para visualizar os detalhes de uma organização, você deve ter as seguintes permissões:

- `organizations:DescribeOrganization`

### AWS Management Console

Para visualizar os detalhes de sua organização

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Navegue até a página Settings (Configurações). Esta página exibe detalhes sobre a organização, incluindo o ID da organização e o nome da conta e o endereço de e-mail atribuídos à conta de gerenciamento da organização.

### AWS CLI & AWS SDKs

Para visualizar os detalhes de sua organização

Você pode usar dos seguintes comandos para visualizar detalhes de uma organização:

- AWS CLI: describe-organization

  O exemplo a seguir mostra as informações incluídas na saída desse comando.

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

> **Important**
>
> O campo `AvailablePolicyTypes` está defasado e não contém informações precisas sobre as políticas habilitadas na sua organização. Para ver a lista precisa e completa dos tipos de política que estão realmente habilitados para a organização, use o comando `ListRoots`, como descrito na parte sobre a AWS CLI da seguinte seção.

- AWS SDKs: DescribeOrganization

## Visualizar os detalhes do contêiner raiz

Ao fazer login na conta de gerenciamento da organização no console do AWS Organizations, você pode visualizar os detalhes do contêiner raiz.

> **Permissões mínimas**
>
> Para visualizar os detalhes da raiz, você deve ter as seguintes permissões:
>
> - `organizations:DescribeOrganization` (somente console)
> - `organizations:ListRoots`

A raiz é o contêiner mais alto na hierarquia de unidades organizacionais (UOs) e geralmente se comporta como uma UO. No entanto, como o contêiner no topo da hierarquia, as alterações na raiz afetam todas as outras UOs e todas as Conta da AWS da organização.

AWS Management Console

Para visualizar detalhes da raiz

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Navegue até o a página Contas da AWS e escolha a UO Raiz (seu nome, não o botão de opção).
3. A página de detalhes Root (Raiz) é exibida e exibe os detalhes da raiz.

AWS CLI & AWS SDKs

Para visualizar detalhes da raiz

Você pode usar um dos seguintes comandos para visualizar detalhes de uma raiz:

- AWS CLI: list-roots

  O exemplo a seguir mostra como recuperar os detalhes da raiz, incluindo quais tipos de política estão habilitados no momento na organização:

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- AWS SDKs: ListRoots

## Visualização de detalhes de uma UO

Quando faz login na conta de gerenciamento da organização no console do AWS Organizations, você pode visualizar os detalhes das UOs de sua organização.

> **Permissões mínimas**
>
> Para visualizar os detalhes de uma unidade organizacional (UO), você deve ter as seguintes permissões:
>
> - `organizations:DescribeOrganizationalUnit`

- `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations
- `organizations:ListOrganizationsUnitsForParent` – necessário somente ao usar o console do Organizations
- `organizations:ListRoots` – necessário somente ao usar o console do Organizations

AWS Management Console

Para visualizar detalhes de uma UO

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, escolha no nome da UO (não no botão) que você deseja examinar. Se a UO desejada for subordinada a outra UO, escolha o ícone de triângulo ao lado da UO pai para expandi-la e ver as UOs do próximo nível da hierarquia. Repita até encontrar a UO desejada.

   A caixa Organizational unit details (Detalhes da unidade organizacional) mostra as informações sobre a UO.

AWS CLI & AWS SDKs

Para visualizar detalhes de uma UO

Você pode usar os seguintes comandos para visualizar detalhes de uma OU:

- AWS CLI, AWS SDKs:
  - list-roots
  - list-children
  - describe-organizational-unit

O exemplo a seguir mostra como encontrar o ID de uma UO usando a AWS CLI. Você encontra o ID da UO atravessando a hierarquia começando com o comando `list-roots` e depois executando `list-children` na raiz e iterativamente em cada um de suas subordinadas até encontrar o que você deseja.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

Depois de ter o ID da UO, o exemplo a seguir mostra como recuperar os detalhes sobre a UO.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- AWS SDKs:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

# Visualizar detalhes de uma conta

Quando faz login na conta de gerenciamento da organização no console do AWS Organizations, você pode visualizar os detalhes sobre suas contas.

**Permissões mínimas**

Para visualizar os detalhes de uma Conta da AWS, você deve ter as seguintes permissões:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations
- `organizations:ListAccounts` – necessário somente ao usar o console do Organizations

AWS Management Console

Para visualizar detalhes de uma Conta da AWS

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Navegue até a página Contas da AWS e escolha o nome do nome da conta (não o botão de opção) que você deseja examinar. Se a conta desejada for subordinada a uma UO, você poderá ter de escolher o ícone de triângulo  ao lado de uma UO para expandi-la e ver suas subordinadas. Repita até encontrar a conta.

   A caixa Account details (Detalhes da conta) mostra as informações sobre a conta.

AWS CLI & AWS SDKs

Para visualizar detalhes de uma Conta da AWS

Você pode usar os seguintes comandos para visualizar detalhes de uma conta:

- AWS CLI:

- list-accounts – lista os detalhes de todas as contas da organização
- describe-account – lista os detalhes apenas da conta especificada

Ambos os comandos retornam os mesmos detalhes para cada conta incluída na resposta.

O exemplo a seguir mostra como recuperar os detalhes sobre uma conta especificada.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
}
```

- AWS SDKs:
  - ListAccounts
  - DescribeAccount

## Visualizar detalhes de uma política

Quando faz login na conta de gerenciamento da organização no console do AWS Organizations, você pode visualizar os detalhes sobre suas políticas.

> **Permissões mínimas**
>
> Para visualizar os detalhes de uma política, você deve ter as seguintes permissões:
>
> - `organizations:DescribePolicy`
> - `organizations:ListPolicies`

### AWS Management Console

Para visualizar os detalhes de uma política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Execute um dos seguintes:
   - Navegue até a página Policies (Políticas) escolha o tipo de política para a política que você deseja examinar.
   - Navegue até a página .Contas da AWS e depois navegue até uma UO ou conta à qual a política está anexada. Por fim, selecione a opção Policies (Políticas) para ver a lista de políticas anexadas.
3. Escolha o no nome da política (não no botão).

   Na página Details (Detalhes) para a política, você pode ver todas as informações sobre a política, incluindo o texto da política JSON e a lista de UOs e contas às quais a política está anexada.

### AWS CLI & AWS SDKs

Para visualizar os detalhes de uma política

Você pode usar um dos seguintes comandos para visualizar detalhes de uma política:

- AWS CLI:
  - list-policies
  - describe-policy – lista os detalhes apenas da política especificada

  O exemplo a seguir mostra como encontrar o ID de política da política que você deseja examinar. Você deve especificar um tipo de política e o comando retorna todas as políticas somente desse tipo.

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
```

```
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

A resposta inclui todos os detalhes, exceto o documento de política JSON.

O exemplo a seguir mostra como recuperar os detalhes apenas da política especificada, incluindo o documento de política JSON.

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":
[\"us-west-2\"]},\"rules\":{\"My-Backup-Rule\"
                    :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-
Backup-Vault\"}}},\"selections\":{\"tags\":{
                    \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
                    My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\"]}}}}}}"
    ]
}
```

- AWS SDKs:
  - ListPolicies
  - DescribePolicy

# Excluir uma organização

Quando você não precisar mais de sua organização, poderá excluí-la. A exclusão de uma organização não encerra a conta de gerenciamento; em vez disso, remove a conta de gerenciamento da organização e exclui a organização em si. A conta de gerenciamento antiga se torna uma Conta da AWS autônoma que não é mais gerenciada pelo AWS Organizations. Você tem três opções: continue a usá-la como uma conta autônoma, use-a para criar outra organização ou aceite um convite de uma organização para entrar como conta-membro.

**Important**

- Se você excluir uma organização, não poderá recuperá-la. Se tiver criado quaisquer políticas dentro da organização, elas também serão excluídas e você não poderá recuperá-las.
- Você pode excluir uma organização somente depois que remover todas as contas-membro da organização. Se você criou algumas de suas contas de associado usando AWS Organizations, poderá ser impedido de remover essas contas. Você só pode remover uma conta-membro se ela tiver todas as informações necessárias para operar como uma Conta da AWS autônoma. Para obter mais informações sobre como fornecer essas informações e remover a conta, consulte Sair de uma organização com sua conta-membro.
- Se você fechou uma conta-membro antes de removê-la da organização, ela entrará em um estado “suspenso” por um período de tempo e você não poderá remover a conta da organização até que ela seja finalmente fechada. Isso pode levar até 90 dias e pode impedir que você exclua a organização até toda as contas-membro serem completamente fechadas.

Quando você remove a conta de gerenciamento de uma organização excluindo a organização, a conta pode ser afetada das seguintes formas:

- A conta é responsável por pagar somente suas próprias cobranças e não é mais responsável pelas cobranças incorridas por qualquer outra conta.
- A integração com outros serviços pode ser desativada. Por exemplo, o AWS IAM Identity Center exige uma organização para operar, portanto, se você remover uma conta de uma organização que oferece suporte ao IAM Identity Center, os usuários nessa conta não poderão mais usar esse serviço.

A conta de gerenciamento de uma organização nunca é afetada por políticas de controle de serviço (SCPs), portanto, não há nenhuma alteração nas permissões depois que as SCPs não estão mais disponíveis.

Tópicos



## Excluir uma organização.

Use o procedimento a seguir para excluir uma organização, o que reverte a conta de gerenciamento antiga para uma Conta da AWS autônoma que não é mais gerenciada pelo AWS Organizations.

> **Permissões mínimas**
>
> Para excluir uma organização, faça login como usuário ou perfil na conta de gerenciamento e verifique se possui as seguintes permissões:
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations

AWS Management Console

Para excluir uma organização

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Antes de excluir a organização, primeiro remova todas as contas da organização. Para obter mais informações, consulte Remover uma conta-membro de sua organização.
3. Navegue até a página Settings (Configurações) e escolha Delete organization (Excluir organização).
4. Na caixa de diálogo Delete organization (Excluir organização), insira o ID da organização que é exibido na linha acima da caixa de texto. Em seguida, escolha Delete organization (Excluir organização).

> **Important**
>
> Essa operação não encerra a conta de gerenciamento, mas a transforma outra vez em uma Conta da AWS autônoma. Para fechar a conta, siga as etapas em Fechar uma conta-membro em sua organização.

AWS CLI & AWS SDKs

Para excluir uma organização

Use um dos seguintes comandos para excluir uma organização:

- AWS CLI: delete-organization

  O exemplo a seguir exclui a organização para a qual a Conta da AWS cujas credenciais são usadas é a conta de gerenciamento.

  ```
  $ aws organizations delete-organization
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: DeleteOrganization

# Gerenciar as Contas da AWS em sua organização

Uma organização é uma coleção de Contas da AWS que você gerencia juntas. Você pode executar as seguintes tarefas para gerenciar as contas que fazem parte da sua organização:

- Visualizar os detalhes das contas da sua organização. Você pode ver o número de ID exclusivo da conta, o Nome de recurso da Amazon (ARN) e as políticas anexadas a eles.
- Exportar uma lista de todas as Contas da AWS da sua organização. Você pode baixar um arquivo .csv de cada conta da sua organização, contendo detalhes sobre ela.
- Convidar Contas da AWS existentes para ingressar na sua organização. Crie convites, gerencie os convites criados e aceite ou recuse convites.
- Criar uma Conta da AWS como parte de sua organização. Criar e acessar uma Conta da AWS que seja automaticamente parte de sua organização.
- Atualize contatos alternativos em sua organização. Atualize contatos alternativos para suas Conta da AWS em sua organização.
- Remover uma Conta da AWS de sua organização. Como administrador da conta de gerenciamento, remova as contas-membro que você não deseja mais gerenciar de sua organização. Administrador da conta de um membro, remova sua conta da organização. Se a conta de gerenciamento tiver anexado uma política à sua conta-membro, você pode ser impedido de remover sua conta.
- Excluir (ou fechar) uma Conta da AWS. Quando você não precisar mais de uma Conta da AWS, pode fechar a conta para evitar qualquer uso ou acúmulo de encargos.

## Impacto de estar em uma organização

- Qual é o impacto para uma Conta da AWS que se conecta a uma organização?
- Qual é o impacto para uma Conta da AWS que você cria em uma organização?

### Impacto para uma Conta da AWS que entra em uma organização?

Quando você convida uma Conta da AWS para participar de uma organização e o proprietário da conta aceita o convite, o AWS Organizations faz automaticamente as seguintes alterações na nova conta-membro:

- O AWS Organizations cria uma função vinculada ao serviço `AWSServiceRoleForOrganizations`. A conta deverá ter essa função se a organização for compatível com todos os recursos. Você só poderá excluir essa função se a organização oferecer suporte apenas ao conjunto de recursos de faturamento consolidado. Se excluir a função e depois você habilitar todos os recursos na organização, o AWS Organizations recriará a função para a conta.
- Você pode ter várias políticas anexadas à raiz da organização ou à UO que contém a conta. Nesse caso, essas políticas se aplicam imediatamente a todos os usuários e funções na conta convidada.
- Você pode habilitar a confiança de serviço para outro serviço da AWS para a sua organização. Desse modo, esse serviço confiável poderá criar funções vinculadas ao serviço ou executar ações em qualquer conta-membro na organização, incluindo em uma conta convidada.

> **Note**
>
> Para contas de membros convidados, AWS Organizations não cria automaticamente a função do IAM OrganizationAccountAccessRole. Essa função concede aos usuários na conta de gerenciamento acesso administrativo à conta-membro. Se quiser habilitar esse nível de controle administrativo sobre uma conta convidada, você pode adicionar manualmente a função. Para ter mais informações, consulte Criando o OrganizationAccountAccessRole em uma conta de membro convidado.

Você pode convidar uma conta para afiliar-se a uma organização que tenha apenas recursos de faturamento consolidado habilitados. Se você quiser habilitar posteriormente todos os recursos para a organização, as contas convidadas devem aprovar a alteração.

## Impacto em uma Conta da AWS criada por você em uma organização?

Quando você cria uma Conta da AWS na sua organização, o AWS Organizations faz automaticamente as seguintes alterações na nova conta-membro:

- O AWS Organizations cria uma função vinculada ao serviço `AWSServiceRoleForOrganizations`. A conta deverá ter essa função se a organização for compatível com todos os recursos. Você só poderá excluir essa função se a organização oferecer suporte apenas ao conjunto de recursos de faturamento consolidado. Se excluir a função e depois você habilitar todos os recursos na organização, o AWS Organizations recriará a função para a conta.

- AWS Organizationscria a função do IAM OrganizationAccountAccessRole. Essa função concede à conta de gerenciamento acesso à nova conta-membro. Embora essa função possa ser excluída, recomendamos que você não o faça para que ela fique disponível como uma opção de recuperação.
- Se você tiver alguma política anexada à raiz da árvore da UO, essa política será aplicada imediatamente a todos os usuários e funções na conta criada. Novas contas são adicionados à UO raiz por padrão.
- Se você tiver habilitado a relação de confiança do serviço para outro serviço da AWS para a sua organização, esse serviço confiável poderá criar funções vinculadas a serviço ou realizar ações em qualquer conta-membro na organização, inclusive na conta criada.

# Convidar um homem Conta da AWS para se juntar à sua organização

Depois de criar uma organização e verificar se você possui o endereço de e-mail associado à conta de gerenciamento, você pode convidar os existentes Contas da AWS para participar da sua organização.

Quando você convida uma conta, AWS Organizations envia um convite para o proprietário da conta, que decide se aceita ou recusa o convite. Você pode usar o AWS Organizations console para iniciar e gerenciar convites enviados para outras contas. Só é possível enviar um convite para outra conta a partir da conta de gerenciamento de sua organização.

> **Note**
>
> O histórico de faturamento e os relatórios de todas as contas permanecem com a conta pagante em uma organização. Antes de mover a conta para uma nova organização, baixe todos os históricos de faturamento e relatório relativos a todas as contas de membro que você queira manter. Isso pode incluir relatórios de custo e uso, relatórios de faturamento detalhados ou relatórios gerados pelo Cost Explorer Service.

Se você for administrador de um Conta da AWS, também poderá aceitar ou recusar um convite de uma organização. Se você aceitar, sua conta passará a ser membro da tal organização. Sua conta somente poderá ingressar em uma organização, portanto, se receber vários convites para ingressar, você só poderá aceitar um.

No momento que uma conta aceita o convite para ingressar em uma organização, a conta de gerenciamento da organização torna-se responsável por todas as cobranças geradas pela nova conta-membro. O método de pagamento anexado à conta-membro deixa de ser usado. Em vez disso, o método de pagamento anexado à conta de gerenciamento da organização paga por todos os encargos acumulados pela conta-membro.

Quando uma conta convidada se junta à sua organização e sua organização está no modo Todos os recursos, a conta de gerenciamento tem acesso administrativo total e controle sobre a conta do membro convidado. No entanto, diferentemente das contas criadas, a função `OrganizationAccountAccessRole` do IAM não é criada automaticamente na conta do membro com permissões para a conta de gerenciamento assumir. Para criar e configurar isso depois que a conta convidada se tornar membro, siga as etapasCriando o OrganizationAccountAccessRole em uma conta de membro convidado.

> **Note**
>
> Quando você cria uma conta na sua organização em vez de convidar uma conta existente para participar, cria AWS Organizations automaticamente uma função do IAM (nomeada `OrganizationAccountAccessRole` por padrão) que você pode usar para conceder aos usuários da conta de gerenciamento acesso à conta criada.

AWS Organizations cria automaticamente uma função vinculada ao serviço nas contas dos membros convidados para apoiar a integração entre outros AWS Organizations AWS serviços. Para ter mais informações, consulte AWS Organizations e funções vinculadas ao serviço.

Para saber o número de convites que você pode enviar por dia, consulte Valores máximo e mínimo. Os convites aceitos não são considerados nessa cota. Assim que um convite é aceito, você pode enviar outro convite no mesmo dia. Cada convite precisa ser respondido dentro de 15 dias, senão ele expira.

Um convite que é enviado a uma conta figura na cota de contas da sua organização. A contagem será restaurada se a conta convidada recusar, a conta de gerenciamento cancelar o convite ou o convite expirar.

Para criar uma conta que faça parte da sua organização automaticamente, consulte Criar uma conta-membro na sua organização.

**Important**

Devido às restrições de cobrança, você pode convidar Contas da AWS somente do mesmo AWS vendedor (no caso da AWS Índia) e AWS dividir como conta de gerenciamento.

- Todas as contas em uma organização devem vir do mesmo vendedor registrado da conta de gerenciamento se a conta de gerenciamento da sua organização tiver sido criada pela Amazon Web Services India Private Limited ("AWS Índia") (anteriormente conhecida como Amazon Internet Services Private Limited). Por exemplo, como AWS vendedor na Índia, você pode convidar somente outras contas AWS indianas para sua organização. Você não pode combinar contas AWS da Índia ou de qualquer outro AWS vendedor.
- Todas as contas em uma organização devem vir da mesma AWS partição da conta de gerenciamento. As contas na Regiões da AWS partição comercial não podem estar em uma organização com contas da partição Regiões da China ou contas na partição AWS GovCloud (US) Regiões.

## Enviar de convites para Contas da AWS

Para convidar contas para a sua organização, primeiro é preciso confirmar que é o proprietário do endereço de e-mail associado à conta de gerenciamento. Para ter mais informações, consulte Verificação do endereço de e-mail. Depois que você tiver verificado o seu endereço de e-mail, conclua as etapas a seguir para convidar contas para a sua organização.

**Permissões mínimas**

Para convidar um Conta da AWS para participar da sua organização, você deve ter as seguintes permissões:

- `organizations:DescribeOrganization` (somente console)
- `organizations:InviteAccountToOrganization`

AWS Management Console

Para convidar outra conta a ingressar na sua organização

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Se você já verificou seu endereço de e-mail com AWS, pule esta etapa.

   Se o seu endereço de e-mail ainda não tiver sido confirmado, siga as instruções no e-mail de verificação em até 24 horas após criar a organização.. Talvez haja um atraso até você receber o e-mail de verificação. Você não poderá convidar uma conta para ingressar na sua organização até verificar o seu endereço de e-mail.
3. Acesse a página Contas da AWS e escolha Adicionar uma conta da AWS .
4. Na página Adicionar uma Conta da AWS, escolha Convidar uma conta da AWS existente.
5. Na AWS página Convidar um existente, em Endereço de e-mail ou ID da conta do Conta da AWS a ser convidado, insira o endereço de e-mail associado à conta a ser convidada ou o número de ID da conta.
6. (Opcional) Em Message to include in the invitation email message (Mensagem a ser incluída na mensagem de e-mail do convite), insira qualquer texto que você queira incluir no convite por e-mail para o proprietário da conta convidada.
7. (Opcional) Na seção Add tags (Adicionar tags), especifique uma ou mais tags que são aplicadas automaticamente à conta depois que seu administrador aceita o convite. Para fazer isso, escolha Add tag (Adicionar tag) e, em seguida, insira uma chave e um valor opcional. Se deixar o valor em branco, ele é definido como uma sequência vazia, não `null`. É possível anexar até 50 tags a uma Conta da AWS.
8. Selecione Send invitation (Enviar convite).

   > **Important**
   >
   > Se você receber uma mensagem de que excedeu as cotas da sua conta da organização ou que não pode adicionar uma conta porque a organização ainda está em inicialização, entre em contato com o AWS Support.
9. O console redireciona você para a página Invitations (Convites), onde você pode ver todos os convites abertos e aceitos aqui. O convite que você acabou de criar aparecerá no topo da lista com o status definido como OPEN (ABERTO).

AWS Organizations envia um convite para o endereço de e-mail do proprietário da conta que você convidou para a organização. Essa mensagem de e-mail inclui um link para o AWS Organizations console, onde o responsável pela conta pode ver os detalhes e optar por aceitar ou recusar o convite. Como alternativa, o proprietário da conta convidada pode ignorar a mensagem de e-mail, acessar diretamente o AWS Organizations console, ver o convite e aceitá-lo ou recusá-lo.

O convite para essa conta é imediatamente considerado na contagem do número máximo de contas que você pode ter em sua organização; o AWS Organizations não aguarda até que a conta aceite o convite. Se a conta convidada negar, a conta de gerenciamento cancelará o convite. Se a conta convidada não responder dentro do período especificado, o convite vai expirar. Em ambos os casos, o convite deixa de ser considerado em sua cota.

AWS CLI & AWS SDKs

Para convidar outra conta a ingressar na sua organização

Você pode usar um dos seguintes comandos para convidar outra conta a ingressar em sua organização:

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
```

```
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```

- AWS SDKs: InviteAccountToOrganization

## Gerenciar convites pendentes para a sua organização

Quando faz login na sua conta de gerenciamento, você pode visualizar todas as Contas da AWS vinculadas em sua organização e cancelar convites pendentes (abertos). Para fazer isso, conclua as seguintes etapas.

**Permissões mínimas**

Para gerenciar convites pendentes para a sua organização, você precisa ter as seguintes permissões:

- `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations
- `organizations:ListHandshakesForOrganization`
- `organizations:CancelHandshake`

### AWS Management Console

Para visualizar ou cancelar convites que são enviados de sua organização para outras contas

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Navegue até a página Invitations (Convites).

   Esta página mostra todos os convites que são enviados de sua organização e seu status atual.

   **Note**

   Convites aceitos, cancelados e recusados continuam aparecendo na lista por 30 dias. Depois disso, elas serão excluídas e não aparecerão mais na lista.

3. Escolha o botão de opção

   ao lado do convite que você deseja cancelar e selecione Cancel invitation (Cancelar convite). Se o botão de opção estiver acinzentado, esse convite não pode ser cancelado.

   O status do convite muda de OPEN (Aberto) para CANCELED (Cancelado).

   AWS envia uma mensagem de e-mail para o proprietário da conta informando que você cancelou o convite. A conta não pode mais participar da organização, a menos que você envie um novo convite.

AWS CLI & AWS SDKs

Para visualizar ou cancelar convites que são enviados de sua organização para outras contas

Você pode usar os seguintes comandos para visualizar ou cancelar convites:

- AWS CLI: list-handshakes-for-organization, cancele o aperto de mão
- O exemplo a seguir mostra os convites enviados por esta organização para outras contas.

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
```

```
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
```

```
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

O exemplo a seguir mostra como cancelar um convite a uma conta.

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
```

```
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS SDKs: ListHandshakesForOrganization, CancelHandshake

## Aceitar ou rejeitar um convite de uma organização

Você Conta da AWS pode receber um convite para participar de uma organização. Você pode aceitar ou recusar o convite. Para fazer isso, conclua as seguintes etapas.

> **Note**
>
> O status de uma conta com uma organização afeta quais dados de custo e uso permanecem visíveis:

- Se uma conta-membro sair de uma organização e se tornar uma conta autônoma, a conta deixará de ter acesso aos dados de custo e uso no período em que a conta era membro da organização. A conta tem acesso apenas aos dados gerados como uma conta autônoma.
- Se uma conta-membro deixar a organização A para entrar na organização B, a conta deixará de ter acesso aos dados de custo e uso do período quando a conta era um membro da organização A. A conta terá acesso apenas aos dados gerados como membro da organização B.
- Se uma conta for associada novamente a uma organização à qual pertencia anteriormente, a conta voltará a ter acesso aos dados de custos e uso históricos.

**Note**

Somente contas-membros e contas independentes podem aceitar ou recusar um convite para participar de uma organização. Se um convite for enviado a uma conta de membro, a mesma deverá sair da organização atual antes de aceitá-lo. Se um convite for enviado para uma conta de gerenciamento que já faz parte de um AWS Organization, essa conta não poderá aceitá-lo até remover todas as contas-membros da organização e excluir a organização.

**Permissões mínimas**

Para aceitar ou recusar um convite para participar de uma AWS organização, você deve ter as seguintes permissões:

- `organizations:ListHandshakesForAccount`— Necessário para ver a lista de convites no AWS Organizations console.
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`— Exigido somente quando aceitar o convite exige a criação de uma função vinculada ao serviço na conta do membro para apoiar a integração com outros AWS serviços. Para ter mais informações, consulte AWS Organizations e funções vinculadas ao serviço.

### AWS Management Console

Para aceitar ou recusar um convite

1. Um convite para participar de uma organização é enviado para o endereço de e-mail do proprietário da conta. Se você for proprietário de uma conta e receber um e-mail de convite, siga as instruções no convite ou acesse o console do AWS Organizations no seu navegador e escolha Invitations (Convites), ou vá direto para a página member account's Invitation (Convite de conta-membro).
2. Se solicitado, faça login na conta de convidado como um usuário IAM, assuma uma função do IAM ou faça login como usuário raiz da conta (não recomendado).
3. A página member account's Invitation (Convite de conta-membro) exibe os convites abertos da sua conta para ingressar em organizações.

   Escolha Accept invitation (Aceitar convite) ou Decline invitation (Recusar convite), conforme apropriado.

   - Se escolher Accept invitation (Aceitar convite) na etapa anterior, o console redirecionará você para a página Organization overview ( Visão geral da organização,) com detalhes sobre a organização da qual sua conta agora é um membro. Você pode visualizar o ID da organização e o endereço de e-mail do proprietário.

     > **Note**
     >
     > Convites aceitos continuam aparecendo na lista por 30 dias. Depois disso, eles serão excluídos e não aparecerão mais na lista.

   AWS Organizations cria automaticamente uma função vinculada ao serviço na nova conta de membro para apoiar a integração entre outros AWS Organizations AWS serviços. Para ter mais informações, consulte AWS Organizations e funções vinculadas ao serviço.

   AWS envia uma mensagem de e-mail para o proprietário da conta de gerenciamento da organização informando que você aceitou o convite. Ela também envia um e-mail para o proprietário da conta-membro informando que a conta agora é um membro da organização.

- Se você escolher Decline (Recusar) na etapa anterior, sua conta permanecerá na página member account's Invitation (Convite de conta-membro), que lista todos os outros convites pendentes.

  AWS envia uma mensagem de e-mail para o proprietário da conta de gerenciamento da organização informando que você recusou o convite.

  > **Note**
  >
  > Convites recusados continuam aparecendo na lista por 30 dias. Depois disso, eles serão excluídos e não aparecerão mais na lista.

AWS CLI & AWS SDKs

Para aceitar ou recusar um convite

Você pode usar os seguintes comandos para aceitar ou recusar um convite:

- AWS CLI: accept-handshake, decline-handshake

  O exemplo a seguir mostra como aceitar um convite para participar de uma organização.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
```

```
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

O exemplo a seguir mostra como recusar um convite para participar de uma organização.

- AWS SDKs: AcceptHandshake, DeclineHandshake

# Criar uma conta-membro na sua organização

Esta página descreve como criar Contas da AWS dentro da sua organização no AWS Organizations. Para saber mais sobre como começar a usar a AWS e como criar uma única Conta da AWS, consulte a Central de recursos de conceitos básicos.

Uma organização é uma coleção de Contas da AWS que você gerencia de forma centralizada. Você pode executar os procedimentos a seguir para gerenciar as contas que fazem parte da sua organização:

- Criação de uma Conta da AWS que seja parte de sua organização
- Acesso à conta-membro que tem uma função de acesso na conta de gerenciamento

**Important**

- Quando você cria uma conta-membro em sua organização, o AWS Organizations cria automaticamente um perfil do AWS Identity and Access Management (IAM) `OrganizationAccountAccessRole` na conta-membro, permitindo que os usuários e perfis na conta de gerenciamento exerçam controle administrativo completo sobre a conta-membro. Essa função está sujeita a todas as políticas de controle de serviço (SCPs) aplicáveis à conta-membro.

  O AWS Organizations também adiciona automaticamente uma política gerenciada com a função `OrganizationAccountAccessRole` à conta-membro. Isso permite o controle centralizado, para que todas as contas adicionais anexadas à mesma política gerenciada sejam atualizadas automaticamente sempre que a política for atualizada. Anteriormente, novas contas criadas em uma organização receberam uma política em linha adicionada que era aplicável somente a essa única conta. Para mais informações sobre políticas em linha e gerenciadas, consulte Managed policies and inline policies (Políticas gerenciadas e políticas em linha) no Guia do usuário do IAM.

  O AWS Organizations também cria automaticamente uma função vinculada ao serviço chamada `AWSServiceRoleForOrganizations` que permite a integração com serviços selecionados da AWS. Você deve configurar os outros serviços para permitir a integração. Para obter mais informações, consulte AWS Organizations e funções vinculadas ao serviço.
- Se esta organização for gerenciada com o AWS Control Tower e criar suas contas usando o Account Factory do AWS Control Tower no console do AWS Control Tower ou APIs. Se você criar uma conta em Organizations (Organizações), essa conta não é inscrita no AWS Control Tower. Para obter mais informações, consulte Referência a recursos fora do AWS Control Tower no Manual do usuário do AWS Control Tower.

> **Note**
>
> As Contas da AWS que você cria como parte de uma organização não são inscritar automaticamente para receber e-mails de marketing da AWS. Para inscrever suas contas para receber e-mails de marketing, consulte https://pages.awscloud.com/communication-preferences.

## Criação de uma Conta da AWS que seja parte de sua organização

Depois de fazer login na conta de gerenciamento da organização, você pode criar contas-membro que são automaticamente parte de sua organização. Ao criar uma conta usando o procedimento a seguir, o AWS Organizations copia automaticamente as seguintes informações de Contato principal da conta de gerenciamento para a nova conta-membro:

- Número de telefone
- Company name (Nome da empresa)
- URL do site
- Endereço

Ele também copia a linguagem de comunicação e as informações do Marketplace (fornecedor da conta em algumas Regiões da AWS) da conta de gerenciamento.

> **Note**
>
> O AWS não coleta automaticamente todas as informações necessárias para uma conta-membro operar como conta independente. Se você precisar remover a conta-membro da organização e torná-la uma conta autônoma, forneça essas informações da conta antes de removê-la. Para obter mais informações, consulte Sair de uma organização com sua conta-membro.

> **Permissões mínimas**
>
> Para criar uma conta membro em sua organização, você deve ter as seguintes permissões:
>
> - `organizations:CreateAccount`

- `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations
- `iam:CreateServiceLinkedRole` (concedido ao principal `organizations.amazonaws.com` para permitir a criação da função vinculada ao serviço necessária nas contas-membro).

### AWS Management Console

Para criar uma Conta da AWS que automaticamente faça parte de sua organização

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, selecione Adicionar uma Conta da AWS.
3. Na página Adicionar uma Conta da AWS, selecione Criar uma Conta da AWS (essa opção é escolhida por padrão).
4. Na página Criar uma Conta da AWS, em Nome da Conta da AWS, insira o nome que deseja atribuir à conta. Esse nome ajuda você a distinguir a conta de todas as outras contas na organização e é distinto do alias do IAM ou do nome do e-mail do proprietário.
5. Para Email address of the account's owner (Endereço de e-mail do proprietário da conta), insira o endereço de e-mail do proprietário da conta. Este endereço de e-mail não pode estar associado a outro Conta da AWS porque se torna a credencial de nome de usuário para o usuário-raiz da conta.
6. (Opcional) Especifique o nome a ser atribuído à função do IAM que é criada automaticamente na nova conta. Essa função concede a permissão à conta de gerenciamento organização para acessar a conta-membro recém-criada. Se você não especificar um nome, o AWS Organizations dará à função o nome padrão de `OrganizationAccountAccessRole`. Recomendamos que você use o nome padrão em todas as contas, por consistência.

> **Important**
>
> Lembre-se do nome do perfil. Você precisará dele posteriormente para conceder acesso à nova conta para usuários e perfis na conta de gerenciamento.

7. (Opcional) Na seção Tags (Tags), adicione uma ou mais tags à nova conta selecionando Add tag (Adicionar tag) e inserindo uma chave e um valor opcional. Se deixar o valor em branco, ele é definido como uma sequência vazia, não `null`. É possível anexar até 50 tags a uma conta.
8. Escolha CreateConta da AWS (Criar).

   - Se você receber um erro indicando que excedeu a cota de conta da organização, consulte Recebo uma mensagem "cota excedida" ao tentar adicionar uma conta à minha organização.
   - Se você receber um erro que indica que você não pode adicionar uma conta porque sua organização ainda está inicializando, aguarde uma hora e tente novamente.
   - Você também pode verificar o log do AWS CloudTrail para saber se a criação da conta foi bem-sucedida. Para obter mais informações, consulte Registrar em log e monitorar no AWS Organizations.
   - Se o erro persistir, entre em contato com o AWS Support.

   A página Contas da AWS é exibida, com a nova conta adicionada à lista.
9. Agora que a conta existe e tem uma função do IAM que concede acesso de administrador aos usuários da conta de gerenciamento, você pode acessar a conta seguindo as etapas em Acessar contas-membro em sua organização.

> **Note**
>
> Quando você cria uma conta, o AWS Organizations inicialmente atribui uma senha longa (64 caracteres), complexa e aleatória para o usuário-raiz. Você não pode recuperar essa senha inicial. Para acessar a conta como o usuário raiz pela primeira vez, você precisa passar pelo processo de recuperação de senha. Para obter mais informações, consulte Acessar a conta-membro como usuário-raiz.

AWS CLI & AWS SDKs

Para criar uma Conta da AWS que automaticamente faça parte de sua organização

Você pode usar um dos seguintes comandos para criar uma conta:

- AWS CLI: create-account

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Você pode verificar o status da criação da conta com o seguinte comando.

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- AWS SDKs: CreateAccount

# Acessar contas-membro em sua organização

Quando você cria uma conta na organização, além do usuário-raiz, o AWS Organizations cria automaticamente uma função do IAM denominada `OrganizationAccountAccessRole` por padrão. Você pode especificar um nome diferente ao criar uma conta, mas, recomendamos usar o nome de modo consistente em todas as suas contas. Fazemos referência ao perfil neste guia pelo nome padrão. O AWS Organizations não cria nenhum outro usuário ou perfil. Para acessar as contas em sua organização, você deve usar um dos seguintes métodos:

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

criar a conta. É altamente recomendável não utilizar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM. Para obter mais recomendações de segurança do usuário raiz, consulte As práticas recomendadas do usuário raiz para a Conta da AWS.

- Se você criar uma conta usando as ferramentas fornecidas como parte do AWS Organizations, poderá acessá-la usando a função pré-configurada denominada `OrganizationAccountAccessRole`, que existe em todas as novas contas criadas dessa maneira. Para ter mais informações, consulte Acesso à conta-membro que tem uma função de acesso na conta de gerenciamento.
- Se você convidar uma conta existente para participar de sua organização e a conta aceitar o convite, poderá optar por criar uma função do IAM que permita o acesso da conta de gerenciamento à conta-membro. Essa função deve ser idêntica à função adicionada automaticamente a uma conta criada com o AWS Organizations. Para criar essa função, consulte Criando o OrganizationAccountAccessRole em uma conta de membro convidado. Depois de criar a função, acesse-a usando as etapas em Acesso à conta-membro que tem uma função de acesso na conta de gerenciamento.
- Use o AWS IAM Identity Center e habilite o acesso confiável para o IAM Identity Center com o AWS Organizations. Isso permite que os usuários façam login no portal de acesso do AWS com suas credenciais corporativas e acessem recursos em suas contas de gerenciamento ou contas-membro designadas.

  Para obter mais informações, consulte Permissões para várias contas no Guia do usuário do AWS IAM Identity Center. Para obter informações sobre como configurar o acesso confiável para o IAM Identity Center, consulte AWS IAM Identity Center e AWS Organizations.

> **Permissões mínimas**
>
> Para acessar uma Conta da AWS a partir de qualquer outra conta de sua organização, você deve ter as seguintes permissões:
>
> - `sts:AssumeRole` – o elemento `Resource` deve ser definido como um asterisco (*) ou o número do ID da conta com o usuário que precisa acessar a nova conta-membro

## Acessar a conta-membro como usuário-raiz

Quando você cria uma nova conta, o AWS Organizations inicialmente atribui uma senha ao usuário raiz com pelo menos 64 caracteres. Todos os caracteres são gerados aleatoriamente sem garantias sobre a aparência de determinados conjuntos de caracteres. Você não pode recuperar essa senha inicial. Para acessar a conta como o usuário raiz pela primeira vez, você precisa passar pelo processo de recuperação de senha. Para obter mais informações, consulte Esqueci minha senha de usuário root Conta da AWS no Guia do usuário de AWSlogin.

Observações

- Como prática recomendada, recomendamos que você não use o usuário raiz para acessar a conta para nada além de criar outros usuários e funções com permissões mais limitadas. Em seguida, faça login como um desses usuários ou funções.
- Recomendamos também que você habilite a autenticação multifator (MFA) no usuário raiz. Redefina a senha e atribua um dispositivo MFA ao usuário raiz.
- Se você criou uma conta-membro em uma organização com um endereço de e-mail incorreto, não poderá fazer login na conta como usuário raiz. Entre em contato com o AWS Billing and Support para obter ajuda.

## Criando o OrganizationAccountAccessRole em uma conta de membro convidado

Por padrão, se você criar a conta-membro como parte de sua organização, a AWS criará automaticamente uma função na conta que concede permissões de administrador aos usuários do IAM na conta de gerenciamento que podem assumir a função. Por padrão, essa função é denominada `OrganizationAccountAccessRole`. Para obter mais informações, consulte Acesso à conta-membro que tem uma função de acesso na conta de gerenciamento.

No entanto, contas de associado que você convida para participar da sua organização não recebem automaticamente a função de administrador criada. Você precisa fazer isso manualmente, como mostrado no procedimento a seguir. Isso duplica a função configurada automaticamente para as contas criadas. Recomendamos que você use o mesmo nome, `OrganizationAccountAccessRole`, para suas funções criadas manualmente, para consistência e facilidade de lembrar.

AWS Management Console

Para criar uma função de administrador do AWS Organizations em uma conta-membro

1. Faça login no console do IAM em https://console.aws.amazon.com/iam/. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta-membro. O usuário ou a função deve ter permissão para criar funções e políticas do IAM.
2. No console do IAM, navegue até Roles e escolha Create role.
3. Escolha e Conta da AWS, em seguida, selecione Outro Conta da AWS.
4. Insira o número de identificação da conta de gerenciamento de 12 dígitos à qual você deseja conceder acesso de administrador. Em Opções, observe o seguinte:
   - Para essa função, porque as contas são internar à empresa, você não deve escolher Require external ID (Requerer ID externo). Para obter mais informações sobre a opção de ID externa, consulte Quando devo usar uma ID externa? no Guia do usuário do IAM.
   - Se tiver MFA habilitado e configurado, você também poderá optar por exigir autenticação usando um dispositivo Multi-Factor Authentication (MFA – Autenticação multifator). Para obter mais informações sobre a MFA, consulte Como usar a autenticação multifator (MFA) AWS no Guia do usuário do IAM.
5. Escolha Próximo.
6. Na página Adicionar permissões, escolha a política AWS gerenciada chamada `AdministratorAccess` e, em seguida, escolha Avançar.
7. Na página Nome, revisão e criação, especifique um nome de função e uma descrição opcional. Recomendamos que você use `OrganizationAccountAccessRole`, para manter a consistência com o nome padrão atribuído à função nas novas contas. Para confirmar as alterações, escolha Criação de função.
8. Sua nova função é exibida na lista de funções disponíveis. Escolha o novo nome da função para ver os detalhes, prestando atenção especial no URL do link que é fornecido. Dê esse URL aos usuários da conta-membro que precisam acessar a função. Além disso, anote o Role ARN (ARN da função), pois você precisará dele na etapa 15.
9. Faça login no console do IAM em https://console.aws.amazon.com/iam/. Dessa vez, faça login como usuário na conta de gerenciamento que tem permissões para criar políticas e atribuí-las a usuários ou grupos.
10. Navegue até Políticas e escolha Criar política.

11. Para Service, escolha STS.
12. Para Actions (Ações), comece digitando **`AssumeRole`** na caixa Filter (Filtro) e marque a caixa de seleção próxima a ela quando aparecer.
13. Em Recursos, certifique-se de que Específico esteja selecionado e escolha Adicionar ARNs.
14. Insira o número do ID da conta-membro da AWS e, depois, o nome da função criada anteriormente nas etapas de 1 a 8. Escolha Add ARNs.
15. Se você estiver concedendo permissão para assumir a função em várias contas membro, repita as etapas 14 e 15 para cada conta.
16. Escolha Próximo.
17. Na página Revisar e criar, insira um nome para a nova política e escolha Criar política para salvar suas alterações.
18. Escolha Grupos de usuários no painel de navegação e, em seguida, escolha o nome do grupo (não a caixa de seleção) que você deseja usar para delegar a administração da conta do membro.
19. Escolha a aba Permissões.
20. Escolha Adicionar permissões, escolha Anexar políticas e, em seguida, selecione a política que você criou nas etapas 11 a 18.

Os usuários que são membros do grupo selecionado agora podem usar os URLs que você capturou na etapa 9 para acessar a função de cada conta membro. Eles podem acessar essas contas membros da mesma forma como acessariam uma conta que você cria na organização. Para obter mais informações sobre como usar a função para administrar uma conta-membro, consulte Acesso à conta-membro que tem uma função de acesso na conta de gerenciamento.

## Acesso à conta-membro que tem uma função de acesso na conta de gerenciamento

Quando você cria a conta-membro usando o console do AWS Organizations, o AWS Organizations cria automaticamente uma função do IAM denominada `OrganizationAccountAccessRole` na conta. Essa função tem permissões administrativas completas na conta do membro. O escopo de acesso para essa função inclui todas as entidades principais na conta de gerenciamento, de modo que a função esteja configurada para conceder esse acesso à conta de gerenciamento da organização. Você pode criar uma função idêntica para a conta de um membro convidado seguindo as etapas de Criando o OrganizationAccountAccessRole em uma conta de membro convidado. Para

usar essa função para acessar a conta-membro, você deve fazer login como usuário a partir da conta de gerenciamento que tem permissão para assumir a função. Para configurar essas permissões, execute o procedimento a seguir. Recomendamos que você conceda permissões a grupos em vez de usuários para a facilidade de manutenção.

AWS Management Console

Para conceder permissões a membros de um grupo do IAM na conta de gerenciamento para acessar a função

1. Faça login no console do IAM em https://console.aws.amazon.com/iam/ como usuário com permissões de administrador na conta de gerenciamento. Isso é necessário para delegar permissões para o grupo do IAM cujos usuários terão acesso à função na conta-membro.
2. Comece criando a política gerenciada de que você precisará posteriormente em ???.

   No painel de navegação, escolha Policies (Políticas) e, em seguida, selecione Create policy (Criar política).
3. Na guia Visual editor (Editor visual), escolha Choose a service (Escolher um serviço), digite **`STS`** na caixa de pesquisa para filtrar a lista e escolha a opção STS.
4. Na seção Ações, digite **`assume`** na caixa de pesquisa para filtrar a lista e escolha a AssumeRoleopção.
5. Na seção Recursos, escolha Específico, escolha Adicionar ARNs e digite o número da conta do membro e o nome da função que você criou na seção anterior (recomendamos nomeá-la`OrganizationAccountAccessRole`).
6. Escolha Adicionar ARNs quando a caixa de diálogo exibir o ARN correto.
7. (Opcional) Se desejar exigir autenticação multifator (MFA) ou restringir o acesso à função a partir de um intervalo de endereços IP especificado, expanda a seção Request conditions (Condições de solicitação) e selecione as opções que deseja impor.
8. Escolha Próximo.
9. Na página Revisar e criar, insira um nome para a nova política. Por exemplo: **`GrantAccessToOrganizationAccountAccessRole`**. Você também pode adicionar uma descrição opcional.
10. Escolha Criar política para salvar a nova política gerenciada.
11. Agora que você tem a política disponível, poderá associá-la a um grupo.

No painel de navegação, escolha Grupos de usuários e, em seguida, escolha o nome do grupo (não a caixa de seleção) cujos membros você deseja que possam assumir a função na conta do membro. Se necessário, você poderá criar outro grupo.

12. Escolha a guia Permissões, escolha Adicionar permissões e depois Anexar políticas.
13. (Opcional) Na caixa Search (Pesquisar), é possível começar a digitar o nome da política para filtrar a lista até ver o nome da política criada em Step 2 até Step 10. Você também pode filtrar todas as políticas AWS gerenciadas escolhendo Todos os tipos e, em seguida, escolhendo Gerenciado pelo cliente.
14. Marque a caixa ao lado da sua política e escolha Anexar políticas.

Os usuários do IAM que são membros do grupo agora têm permissões para alternar para a nova função no console do AWS Organizations seguindo o procedimento abaixo.

AWS Management Console

Para alternar para a função para a conta-membro

Ao usar a função, o usuário tem permissões de administrador na nova conta-membro. Instrua os usuários do IAM que são membros do grupo a fazer o seguinte para alternar para a nova função.

1. No canto superior direito do console do AWS Organizations, selecione o link que contém seu nome de login atual e escolha Switch role (Alternar função).
2. Insira o nome da função e o número do ID da conta fornecida pelo administrador.
3. Em Display Name (Nome de exibição), insira o texto a ser exibido na barra de navegação no canto superior direito em vez do seu nome de usuário enquanto estiver usando a função. Você também pode escolher uma cor.
4. Selecione Switch Role (Mudar de função). Agora, todas as ações que você executar serão feitas com as permissões concedidas à função para a qual você mudou. Você não tem mais as permissões associadas ao seu usuário original do IAM até você alternar de volta.
5. Ao concluir as ações que exigem as permissões da função, você poderá alternar de volta para seu usuário do IAM normal. Escolha o nome da função no canto superior direito (o que você especificou como Nome de Exibição) e, em seguida, escolha Voltar para. *UserName*

### Recursos adicionais

- Para obter mais informações sobre como conceder permissões para trocar de função, consulte Conceder permissões a um usuário para trocar de função no Guia do usuário do IAM.
- Para obter mais informações sobre o uso de uma função que você recebeu permissão para assumir, consulte Mudança para uma função (console) no Guia do usuário do IAM.
- Para ver um tutorial sobre o uso de funções para acesso entre contas, consulte Tutorial: Delegar acesso Contas da AWS usando funções do IAM no Guia do usuário do IAM.
- Para obter informações sobre fechamento de Contas da AWS, consulte Fechar uma conta-membro em sua organização.

## Exportar detalhes da Conta da AWS da organização

Com o AWS Organizations, os usuários da conta de gerenciamento e os administradores delegados de uma organização podem exportar um arquivo .csv com todos os detalhes de conta de uma organização. Fazendo isso, fica fácil para os administradores da organização visualizar contas e filtrar por status: `ACTIVE`, `SUSPENDED`, ou `PENDING`. Se sua organização tiver muitas contas, a opção de download de arquivo .csv facilitará a visualização e a classificação dos detalhes de conta em uma planilha.

Anteriormente, a única maneira de visualizar contas era examinando a hierarquia de contas ou a exibição da lista no console do AWS Organizations.

> **Note**
>
> Somente as entidades principais na conta de gerenciamento podem baixar a lista de contas.

### Exportar uma lista de todas as Contas da AWS da sua organização.

Ao fazer login na conta de gerenciamento da organização, você pode obter uma lista de todas contas que fazem parte da sua organização em um arquivo .csv. A lista contém detalhes individuais da conta, mas não especifica a qual unidade organizacional (UO) a conta pertence.

O arquivo .csv contém as seguintes informações para cada conta:

- ID da conta - identificador numérico da conta. Por exemplo: 123456789012

- ARN - nome de recurso da Amazon da conta. Por exemplo: `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`.
- E-mail - o endereço de e-mail associado à conta. Por exemplo: marymajor@example.com
- Nome - nome da conta fornecido pelo criador dela. Por exemplo: stage testing account
- Status - status da conta dentro da organização. Os valores podem ser `PENDING`, `ACTIVE` ou `SUSPENDED`.
- Método de ingresso - especifica como a conta foi criada. O valor pode ser `INVITED` ou `CREATED`.
- Timestamp do ingresso - data e hora em que a conta ingressou na organização.

> **Permissões mínimas**
>
> Para exportar um arquivo .csv com todas as contas-membro da sua organização, você precisa ter as seguintes permissões:
>
> - `organizations:DescribeOrganization`
> - `organizations:ListAccounts`

AWS Management Console

Para exportar um arquivo .csv para todas as Contas da AWS da sua organização

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Selecione Actions (Ações) e, na Conta da AWS, escolha Export account list (Exportar lista de contas). O banner azul no topo da página indica "Export is in progress!" (A exportação está em andamento!).
3. Quando o arquivo fica pronto, o banner fica verde e indica: "Download is ready!" (O download está pronto!). Escolha Download CSV (Baixar CSV). O arquivo `Organization_accounts_information.csv` é baixado no seu dispositivo.

AWS CLI & AWS SDKs

A única maneira de exportar o arquivo .csv com detalhes de conta é usando o AWS Management Console. Não há como exportar o arquivo .csv da lista de contas usando o AWS CLI.

# Remover uma conta-membro de sua organização

Parte do gerenciamento de contas em uma organização é remover contas-membro que não são mais necessárias. A remoção de uma conta-membro não encerra a conta, mas remove a conta-membro da organização. A conta do antigo membro se torna uma Conta da AWS autônoma que não é mais gerenciada pelo AWS Organizations. Em seguida, a conta não estará mais sujeita a nenhuma política e será responsável por seus próprios pagamentos de contas. A conta de gerenciamento da organização não é mais cobrada por nenhuma despesa acumulada pela conta após sua remoção da organização.

Para obter informações sobre como remover a conta de gerenciamento, consulte Excluir uma organização.

Tópicos



## Considerações antes de remover uma conta de uma organização

Antes de remover uma conta, é importante saber o seguinte:

- Você pode remover uma conta de sua organização somente se a conta tem as informações necessárias para operar como uma conta autônoma. Ao criar uma conta em uma organização usando o console do AWS Organizations, a API ou os comandos da AWS CLI, todas as informações exigidas das contas independentes não são coletadas automaticamente. Para cada conta que você desejar tornar autônoma, é necessário escolher um plano de suporte, fornecer e confirmar as informações de contato exigidas, bem como informar o método de pagamento atual. A AWS usa o método de pagamento para cobrar qualquer atividade faturável (fora do nível gratuito da AWS) da AWS que ocorra enquanto a conta não estiver anexada a uma organização. Para remover uma conta que ainda não tem essas informações, siga as etapas em Sair de uma organização com sua conta-membro.
- Para remover uma conta que você criou na organização, você deve aguardar pelo menos sete dias após a criação da conta. As contas convidadas não estão sujeitas a esse período de espera.

- No momento em que a conta sai com sucesso da organização, o proprietário da Conta da AWS torna-se responsável por todos os novos custos acumulados da AWS, e o método de pagamento da conta é usado. A conta de gerenciamento da organização não é mais responsável.
- A conta que você deseja remover não deve ser uma conta de administrador delegado para qualquer serviço da AWS habilitado para sua organização. Se a conta for um administrador delegado, você deve primeiro alterar a conta de administrador delegado para outra conta que esteja permanecendo na organização. Para obter mais informações sobre como desabilitar ou alterar a conta de administrador delegado para um serviço da AWS, consulte a documentação desse serviço.
- Mesmo depois da remoção das contas criadas (contas criadas usando o console do AWS Organizations ou a API `CreateAccount`) de uma organização, (i) as contas criadas serão regidas pelos termos de criação do contrato da conta de gerenciamento conosco e (ii) a criação da conta de gerenciamento permanecerá conjunta e solidariamente responsável por quaisquer ações executadas pelas contas criadas. Os contratos dos clientes conosco e os direitos e obrigações sob esses acordos não podem ser atribuídos ou transferidos sem nosso consentimento prévio. Para obter nosso consentimento, entre em contato com a AWS.
- Quando uma conta membro deixa uma organização, essa conta deixa de ter acesso aos dados de custo e uso no período quando a conta era membro da organização. No entanto, a conta de gerenciamento da organização ainda pode acessar os dados. Se reentrar na organização, a conta poderá acessar novamente esses dados.
- Quando uma conta-membro sai de uma organização, todas as tags anexadas à conta são excluídas.
- Quando você remove uma conta de membro da organização, qualquer perfil do IAM criado para permitir o acesso pela conta de gerenciamento da organização não é excluído automaticamente. Se você deseja terminar esse acesso a partir da conta de gerenciamento da antiga organização, exclua manualmente o perfil do IAM. Para obter mais informações sobre como excluir uma função, consulte Excluir funções ou perfis de instância no Guia do usuário do IAM.

## Efeitos de remover uma conta de uma organização

Quando você remove uma conta de uma organização, nenhuma alteração direta é feita na conta. No entanto, os seguintes efeitos indiretos ocorrem:

- A conta agora é responsável por pagar suas próprias cobranças e deve ter um método de pagamento válido anexado.

- As entidades primárias da conta não são mais afetadas pelas políticas que se aplicavam na organização. Isso significa que as restrições impostas por SCPs são removidas, e os usuários e as funções da conta podem ter mais permissões do que tinham antes. Outros tipos de política da organização não podem mais ser aplicados ou processados.
- Se usar a chave de condição `aws:PrincipalOrgID` em qualquer política para restringir o acesso apenas aos usuários e funções das Contas da AWS de sua organização, você deve revisar e, possivelmente, atualizar essas políticas antes de remover a conta-membro. Se você não atualizar as políticas, os usuários e funções na conta podem perder o acesso aos recursos quando a conta sair da organização.
- A integração com outros serviços pode ser desativada. Se você remover uma conta de uma organização que tem integração com um serviço da AWS, os usuários dessa conta não poderão mais usar esse serviço.

## Remover uma conta-membro da sua organização

Quando faz login na conta de gerenciamento da organização, você pode remover contas-membro da organização que não são mais necessárias. Para fazer isso, conclua o seguinte procedimento. Este procedimento se aplica somente a contas-membro. Para remover a conta de gerenciamento, é necessário excluir a organização.

> **Note**
>
> Se uma conta-membro for removida de uma organização, ela não será mais coberta pelos contratos da organização. Os administradores das contas de gerenciamento deverão informar às contas-membro antes de removê-las da organização, para que elas possam colocar novos contratos em vigor, se necessário. Uma lista de contratos ativos da organização pode ser visualizada no console do AWS Artifact na página AWS Artifact Organization Agreements (Contratos da organização do AWS Artifact).

> **Permissões mínimas**
>
> Para remover uma ou mais contas-membro de sua organização, você deve fazer login como um usuário ou perfil na conta de gerenciamento com as seguintes permissões:
>
> - `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations

- `organizations:RemoveAccountFromOrganization`

Se você optar por fazer login como um usuário ou perfil em uma conta-membro na etapa 5, esse usuário ou perfil deverá ter as seguintes permissões:

- `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations.
- `organizations:LeaveOrganization` – observe que o administrador da organização pode aplicar uma política para a sua conta que remove essa permissão, impedindo que você remova sua conta da organização.
- Se quando você fizer login como usuário do IAM estiverem faltando informações de pagamento na conta, será necessário que o usuário tenha as permissões `aws-portal:ModifyBilling` e `aws-portal:ModifyPaymentMethods` (caso a conta ainda não tenha migrado para permissões refinadas) OU as permissões `payments:CreatePaymentInstrument` e `payments:UpdatePaymentPreferences` (caso a conta já tenha migrado para permissões refinadas). Além disso, a conta-membro precisa ter acesso de usuário do IAM ao faturamento habilitado. Se ele ainda não estiver habilitado, consulte Ativar o acesso ao console do Billing and Cost Management no Guia do usuário do AWS Billing.

AWS Management Console

Para remover uma conta-membro da sua organização

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, encontre e escolha a caixa de seleção☑ próxima à conta-membro que você deseja remover de sua organização. Você pode navegar na hierarquia da UO ou habilitar View Contas da AWS only (Exibir apenas Contas da AWS) para ver uma lista simples de contas sem a estrutura da UO. Se você tiver muitas contas, talvez seja necessário escolher Load more accounts in 'ou-name' (Carregar mais contas em ‘nome-uo’) no fim da lista para encontrar todas que você deseja mover.

Na página Contas da AWS, encontre e escolha o nome próximo à conta-membro que você deseja remover de sua organização. Talvez seja necessário expandir as UOs (escolha  ) para encontrar a conta que você deseja.

3. Selecione Actions (Ações), então, em Conta da AWS, escolha Remove from organization (Remover da organização).
4. No diálogo Remove account 'account-name' (#account-id-num) from organization? (Remover conta 'account-name'(#account-id-num) da organização?, escolha Remove Account (Remover conta).
5. Se o AWS Organizations não conseguir remover uma ou mais contas, isso será normal porque você não forneceu todas as informações necessárias para a conta funcionar como uma conta autônoma. Siga estas etapas:

   a. Faça login na conta com falha. Recomendamos fazer login na conta-membro escolhendo Copy link (Copiar link) e colando-o na barra de endereço de uma nova janela de navegação incógnito. Se você não usar uma janela incognito, será desconectado da conta de gerenciamento e não poderá navegar de volta para essa caixa de diálogo.

   b. O navegador leva você diretamente para o processo de cadastramento para concluir as etapas ausentes para essa conta. Conclua todas as etapas apresentadas. Isso pode incluir o seguinte:

      - Fornecer informações de contato
      - Fornecer um método de pagamento válido
      - Verificar o número de telefone
      - Selecionar uma opção de plano de suporte

   c. Depois que você conclui a última etapa do cadastramento, a AWS redireciona automaticamente o navegador para o console do AWS Organizations para a conta membro. Escolha Leave organization e, em seguida, confirme sua escolha na caixa de diálogo de confirmação. Você será redirecionado para a página Getting Started (Conceitos básicos) do console do AWS Organizations, onde você pode visualizar convites pendentes para a sua conta para ingressar em outras organizações.

   d. Remova as funções do IAM que concedem acesso à sua conta a partir da organização.

> **Important**
>
> Se a conta foi criada na organização, o Organizations criou automaticamente uma função do IAM na conta que habilitou o acesso pela conta de gerenciamento da organização. Se a conta foi convidada para participar, então o Organizations não criou automaticamente essa função, mas você ou outro administrador pode ter criado uma para obter os mesmos benefícios. Em ambos os casos, quando você remove a conta da organização, essa função não é excluída automaticamente. Se você deseja terminar esse acesso a partir da conta de gerenciamento da antiga organização, exclua manualmente essa função do IAM. Para obter mais informações sobre como excluir uma função, consulte Excluir funções ou perfis de instância no Guia do usuário do IAM.

AWS CLI & AWS SDKs

Para remover uma conta-membro da sua organização

Você pode usar um dos seguintes comandos para remover uma conta-membro:

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS SDKs: RemoveAccountFromOrganization

Depois que a conta-membro for removida da organização, certifique-se de remover da organização as funções do IAM que concedem acesso à sua conta.

> **Important**
>
> Se a conta foi criada na organização, o Organizations criou automaticamente uma função do IAM na conta que habilitou o acesso pela conta de gerenciamento da organização. Se a conta foi convidada para participar, então o Organizations não criou automaticamente essa função, mas você ou outro administrador pode ter criado uma para obter os mesmos

benefícios. Em ambos os casos, quando você remove a conta da organização, essa função não é excluída automaticamente. Se você deseja terminar esse acesso a partir da conta de gerenciamento da antiga organização, exclua manualmente essa função do IAM. Para obter mais informações sobre como excluir uma função, consulte Excluir funções ou perfis de instância no Guia do usuário do IAM.

Em vez disso, as contas-membro podem remover a si mesmas utilizando leave-organization. Para obter mais informações, consulte Sair de uma organização com sua conta-membro.

## Sair de uma organização com sua conta-membro

Quando faz login em uma conta-membro, você pode remover essa conta de sua organização. Para fazer isso, conclua o seguinte procedimento. Este procedimento se aplica somente a contas-membro. A conta de gerenciamento não pode deixar a organização usando essa técnica. Para remover a conta de gerenciamento, é necessário excluir a organização.

**Note**

O status de uma conta com uma organização afeta quais dados de custo e uso permanecem visíveis:

- Se uma conta-membro sair de uma organização e se tornar uma conta autônoma, a conta deixará de ter acesso aos dados de custo e uso no período em que a conta era membro da organização. A conta tem acesso apenas aos dados gerados como uma conta autônoma.
- Se uma conta-membro deixar a organização A para entrar na organização B, a conta deixará de ter acesso aos dados de custo e uso do período quando a conta era um membro da organização A. A conta terá acesso apenas aos dados gerados como membro da organização B.
- Se uma conta for associada novamente a uma organização à qual pertencia anteriormente, a conta voltará a ter acesso aos dados de custos e uso históricos.

**Important**

Se você sair de uma organização, não está mais coberto pelos contratos da organização que foram aceitos em seu nome pela conta de gerenciamento da organização. Você pode

ver uma lista desses contratos da organização no console do AWS Artifact, na página AWS Artifact Organization Agreements (Contratos da organização do AWS Artifact). Antes de deixar a organização, você deve determinar (com a ajuda da equipe jurídica, de privacidade ou de conformidade, se adequado) se é necessário ter novos contratos em vigor.

Permissões mínimas

Para sair de uma organização AWS você deve ter as seguintes permissões:

- `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations.
- `organizations:LeaveOrganization` – observe que o administrador da organização pode aplicar uma política para a sua conta que remove essa permissão, impedindo que você remova sua conta da organização.
- Se quando você fizer login como usuário do IAM estiverem faltando informações de pagamento na conta, será necessário que o usuário tenha as permissões `aws-portal:ModifyBilling` e `aws-portal:ModifyPaymentMethods` (caso a conta ainda não tenha migrado para permissões refinadas) OU as permissões `payments:CreatePaymentInstrument` e `payments:UpdatePaymentPreferences` (caso a conta já tenha migrado para permissões refinadas). Além disso, a conta-membro precisa ter acesso de usuário do IAM ao faturamento habilitado. Se ele ainda não estiver habilitado, consulte Ativar o acesso ao console do Billing and Cost Management no Guia do usuário do AWS Billing.

AWS Management Console

Para sair de uma organização com sua conta-membro

1. Faça login no console do AWS Organizations no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta-membro.

   Por padrão, você não tem acesso à senha do usuário raiz em uma conta de associado criada usando AWS Organizations. Se necessário, recupere a senha do usuário raiz seguindo as etapas em Acessar a conta-membro como usuário-raiz.

2. Na página Painel do Organizations, escolha Sair da organização.
3. Na caixa de diálogo Confirmar saída da organização?, escolha Sair da organização. Quando solicitado, confirme sua escolha para remover a conta. Após a confirmação, você será redirecionado para a página Conceitos básicos do console do AWS Organizations, onde poderá visualizar convites pendentes para a sua conta ingressar em outras organizações.

   Se você receber uma mensagem Ainda não é possível sair da organização, sua conta não tem todas as informações necessárias para operar como uma conta independente. Se este for o caso, vá para a próxima etapa.
4. Se a caixa de diálogo Confirmar a saída da organização? exibir a mensagem Ainda não é possível sair da organização, escolha o link Concluir as etapas de inscrição da conta.
5. Na página Inscrever-se na AWS, insira todas as informações necessárias para que essa se torne uma conta independente. Isso pode incluir os seguintes tipos de informações:

   - Nome e endereço de contato
   - Método de pagamento válido
   - Verificação de número de telefone
   - Opções do plano de suporte
6. Quando for exibida a caixa de diálogo informando que o processo de cadastramento foi concluído, escolha Leave organization.

   Uma caixa de diálogo de confirmação é exibida. Confirme sua escolha para remover a conta. Você será redirecionado para a página Getting Started (Conceitos básicos) do console do AWS Organizations, onde você pode visualizar convites pendentes para a sua conta para ingressar em outras organizações.
7. Remova as funções do IAM que concedem acesso à sua conta a partir da organização.

   **Important**

   Se a conta foi criada na organização, o Organizations criou automaticamente uma função do IAM na conta que habilitou o acesso pela conta de gerenciamento da organização. Se a conta foi convidada para participar, então o Organizations não criou automaticamente essa função, mas você ou outro administrador pode ter criado uma para obter os mesmos benefícios. Em ambos os casos, quando você remove a conta da organização, essa função não é excluída automaticamente. Se você deseja terminar esse acesso a partir da conta de gerenciamento da antiga

organização, exclua manualmente essa função do IAM. Para obter mais informações sobre como excluir uma função, consulte Excluir funções ou perfis de instância no Guia do usuário do IAM.

AWS CLI & AWS SDKs

Para sair de uma organização como uma conta-membro

Você pode usar um dos seguintes comandos para sair de uma organização:

- AWS CLI:leave-organization

  O exemplo a seguir faz com que a conta cujas credenciais são usadas para executar o comando saia da organização.

  ```
  $ aws organizations leave-organization
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS SDKs: LeaveOrganization

Depois que a conta-membro sair da organização, certifique-se de remover da organização as funções do IAM que concedem acesso à sua conta.

> **Important**
>
> Se a conta foi criada na organização, o Organizations criou automaticamente uma função do IAM na conta que habilitou o acesso pela conta de gerenciamento da organização. Se a conta foi convidada para participar, então o Organizations não criou automaticamente essa função, mas você ou outro administrador pode ter criado uma para obter os mesmos benefícios. Em ambos os casos, quando você remove a conta da organização, essa função não é excluída automaticamente. Se você deseja terminar esse acesso a partir da conta de gerenciamento da antiga organização, exclua manualmente essa função do IAM. Para obter mais informações sobre como excluir uma função, consulte Excluir funções ou perfis de instância no Guia do usuário do IAM.

As contas-membro também podem ser removidas por um usuário na conta de gerenciamento usando remove-account-from-organization. Para obter mais informações, consulte Remover uma conta-membro da sua organização.

# Fechar uma conta-membro em sua organização

Se você não precisar mais de uma conta de membro em sua organização, poderá fechá-la no AWS Organizations console seguindo as instruções nesta seção. Você só pode fechar uma conta de membro usando o AWS Organizations console se sua organização estiver no modo Todos os recursos.

Você também pode fechar um Conta da AWS diretamente da página Conta AWS Management Console após fazer login como usuário root. Para step-by-step obter instruções, consulte Fechar um Conta da AWS no Guia de gerenciamento de AWS contas.

Para fechar uma conta de gerenciamento, consulteFechando uma conta de gerenciamento em sua organização.

## Como fechar uma conta-membro

Quando você acessa a conta de gerenciamento da organização, é possível encerrar contas-membro que fazem parte de sua organização. Para fazer isso, conclua as seguintes etapas.

> **Important**
>
> Antes de fechar sua conta de membro, é altamente recomendável que você analise as considerações e entenda o impacto do fechamento de uma conta. Para obter mais informações, consulte O que você precisa saber antes de fechar sua conta e O que esperar depois de fechar sua AWS conta no Guia de gerenciamento de contas.

AWS Management Console

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

1. Faça login no console do AWS Organizations.
2. Na página Contas da AWS, localize e escolha o nome da conta-membro que deseja encerrar. É possível navegar na hierarquia da UO ou ver uma lista simples de contas sem a estrutura da UO.

3. Selecione Close (Encerrar) ao lado do nome da conta na parte superior da página. Organizações no modo de cobrança consolidada não conseguirão ver o botão Fechar no console. Para fechar uma conta no modo de cobrança consolidada, siga as etapas na guia Conta autônoma em Como fechar sua conta no Guia de gerenciamento de AWS contas.
4. Marque cada caixa de seleção para confirmar todas as declarações necessárias para o encerramento de conta.
5. Insira o ID da conta do membro e escolha Fechar conta.

> **Note**
>
> Qualquer conta de membro que você fechar exibirá uma `SUSPENDED` etiqueta ao lado do nome da conta no AWS Organizations console.

Para fechar uma conta de membro na página Contas

Opcionalmente, você pode fechar uma conta de AWS membro diretamente da página Contas no AWS Management Console. Para step-by-step obter orientação, siga as instruções em Fechar e Conta da AWS no Guia de gerenciamento de AWS contas.

AWS CLI & AWS SDKs

Para fechar um Conta da AWS

Você pode usar um dos seguintes comandos para encerrar uma conta da AWS :

- AWS CLI: close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: CloseAccount

## Como proteger contas-membro contra o fechamento

Para proteger uma conta-membro o fechamento acidental, você pode criar uma política do IAM para especificar quais contas são isentas de fechamento. Não é possível encerrar nenhuma conta-

membro protegida com essas políticas. Também não é possível fazer isso usando uma SCP, pois elas não afetam entidades principais na conta de gerenciamento.

Há duas maneiras de criar uma política do IAM que recuse o encerramento de contas:

- Listar explicitamente na política cada conta que deseja proteger incluindo o `arn` no elemento `Resource`. Para ver um exemplo, consulte Impedir que as contas-membro listadas nesta política sejam fechadas.
- Etiquetar contas individuais para impedir que elas sejam encerradas. Use a chave de condição global da etiqueta `aws:ResourceTag` em sua política para evitar que qualquer conta com a etiqueta seja encerrada. Para saber como etiquetar uma conta, consulte Etiquetar recursos do Organizations. Para ver um exemplo, consulte Impedir que contas-membro com tags sejam fechadas .

## Exemplos de políticas do IAM que impedem fechamentos de contas-membro

Os exemplos de código a seguir mostram dois métodos diferentes que você pode usar para impedir que as contas dos membros fechem suas contas.

Impedir que contas-membro com tags sejam fechadas

É possível anexar a seguinte política a uma identidade na sua conta de gerenciamento. Essa política impede que as entidades principais na conta de gerenciamento encerrem qualquer conta-membro que esteja marcada com a chave de condição global da etiqueta `aws:ResourceTag`, a chave `AccountType` e o valor de chave `Critical`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

Impedir que as contas-membro listadas nesta política sejam fechadas

É possível anexar a seguinte política a uma identidade na sua conta de gerenciamento. Essa política impede que entidades principais na conta de gerenciamento encerrem contas-membro especificadas no elemento `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

# Fechando uma conta de gerenciamento em sua organização

Para fechar a conta de gerenciamento em sua organização, você deve primeiro fechar ou remover todas as contas de membros na organização. O ato de fechar a conta de gerenciamento também exclui a instância AWS Organizations e todas as políticas que você criou dentro dessa organização após o término do período pós-encerramento.

## Como fechar uma conta de gerenciamento

Use o procedimento a seguir para fechar uma conta de gerenciamento.

> **Important**
>
> Antes de fechar sua conta de gerenciamento, é altamente recomendável que você analise as considerações e entenda o impacto do fechamento de uma conta. Para obter mais informações, consulte O que você precisa saber antes de fechar sua conta e O que esperar depois de fechar sua AWS conta no Guia de gerenciamento de contas.

AWS Management Console

Para fechar uma conta de gerenciamento na página Contas

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

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

AWS CLI & AWS SDKs

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

# Atualizar contatos alternativos em sua organização

Você pode atualizar contatos alternativos para contas dentro de sua organização usando o console do AWS Organizations ou programaticamente via AWS CLI do AWS SDKs. Para saber como atualizar contatos alternativos, consulte Acessar ou atualizar os contatos alternativos na Referência do gerenciamento de contas da AWS.

# Atualizar informações de contato principal em sua organização

Você pode atualizar as informações de contato principal para contas dentro de sua organização usando o console do AWS Organizations ou programaticamente por meio da AWS CLI ou AWS SDKs. Para saber como atualizar as informações de contato principal, consulte Accessing or updating the primary account contact (Acessar ou atualizar o contato da conta principal) na Referência de gerenciamento de contas da AWS.

# Atualização das Regiões da AWS habilitadas em sua organização

É possível atualizar as Regiões da AWS habilitadas para contas em sua organização usando o console do AWS Organizations. Para saber como atualizar as Regiões da AWS habilitadas, consulte Specifying which Regiões da AWS your account can use (Como especificar quais Regiões da AWS sua conta pode usar) na AWS Account Management Reference (Referência para gerenciamento de contas do AWS).

# Gerenciando políticas em AWS Organizations

As políticas AWS Organizations permitem que você aplique tipos adicionais de gerenciamento ao Contas da AWS em sua organização. Você pode usar políticas quando todos os recursos estão habilitados na sua organização.

O AWS Organizations console exibe o status de habilitado ou desativado para cada tipo de política. Na guia Organizar contas, escolha `Root`, no painel de navegação à esquerda. O painel de detalhes no lado direito da tela mostra todos os tipos de política disponíveis. A lista indica quais estão ativados e quais estão desativados na raiz da organização em questão. Se a opção para Ativar um tipo estiver presente, isso significa que esse tipo está desativado. Se a opção para Desativar um tipo estiver presente, isso significa que esse tipo está ativado.

## Tipos de políticas

O Organizations oferece tipos de política nas duas categorias amplas a seguir:

### Políticas de autorização

As políticas de autorização ajudam a gerenciar centralmente a segurança das Contas da AWS em sua organização.

- As políticas de controle de serviço (SCPs) oferecem controle central sobre as permissões máximas disponíveis para todas as contas da organização.

### Políticas de gerenciamento

As políticas de gerenciamento permitem que você configure e gerencie centralmente AWS os serviços e seus recursos.

- As políticas de exclusão dos serviços de Inteligência Artificial (IA) permitem que você controle a coleta de dados para os serviços de IA da AWS para todas as contas de sua organização.
- As políticas de backup ajudam você a gerenciar e aplicar centralmente os planos de backup aos AWS recursos nas contas da sua organização.
- As políticas de tags ajudam você a padronizar as tags anexadas aos AWS recursos nas contas da sua organização.

A tabela a seguir resume algumas das características de cada tipo de política. Para obter características adicionais sobre esses tipos de políticas, consulte Cotas para AWS Organizations.

| Tipo de política | Afeta a conta de gerenciamento | Número máximo que você pode anexar a uma raiz, UO ou conta | Tamanho máximo | Suporta a exibição das políticas em vigor para UO ou conta |
|---|---|---|---|---|
| SCP |  Não | 5 | 2500 caracteres |  Não |
| Política de cancelamento de serviços de IA |  sim | 5 | 2500 caracteres |  sim |
| Política de backup |  sim | 10 | 10 mil caracteres |  sim |
| Política de tag |  Sim | 10 | 10 mil caracteres |  Sim |

## Usar políticas na organização

- Habilitar e desabilitar tipos de política
- Obter informações sobre as políticas da sua organização
- Administrador delegado para AWS Organizations
- Políticas de gerenciamento

- Políticas de controle de serviço (SCPs)

# Habilitar e desabilitar tipos de política

## Habilitação de um tipo de política

Antes de criar e anexar uma política à sua organização, é necessário habilitar esse tipo de política para uso. Habilitar um tipo de política é uma tarefa única na raiz da organização. É possível habilitar um tipo de política somente da conta de gerenciamento da organização.

> **Permissões mínimas**
>
> Para habilitar um tipo de política, você precisa de permissão para executar as seguintes ações:
>
> - `organizations:EnablePolicyType`
> - `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations
> - `organizations:ListRoots` – necessário somente ao usar o console do Organizations

AWS Management Console

Para habilitar um tipo de política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Policies (Políticas), escolha o nome do tipo de política que você deseja habilitar.
3. Na página do tipo de política, escolha Habilitar ***tipo de política***.

   A página é substituída por uma lista das políticas disponíveis do tipo especificado.

AWS CLI & AWS SDKs

Para habilitar um tipo de política

É possível usar uma das seguintes opções para habilitar um tipo de política:

- AWS CLI: enable-policy-type

  O exemplo a seguir mostra como habilitar políticas de backup para sua organização. Observe que você deve especificar o ID da raiz da organização.

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

  A lista de `PolicyTypes` na saída agora inclui o tipo de política especificado com o `Status` de `ENABLED`.

- AWS SDKs: EnablePolicyType

## Desabilitar um tipo de política

Se não quiser mais usar determinado tipo de política em sua organização, você poderá desabilitar esse tipo para impedir seu uso acidental. É possível desabilitar um tipo de política somente da conta de gerenciamento da organização.

> **Important**
>
> - Ao desabilitar um tipo de política, todas as políticas do tipo especificado são automaticamente desanexadas de todas as entidades na raiz da organização. As políticas não são excluídas.
> - (Somente tipo política de controle de serviço) Se você habilitar novamente o tipo de política SCP posteriormente, todas as entidades na raiz da organização serão inicialmente

anexadas apenas à SCP `FullAWSAccess` padrão. As anexações de SCPs a entidades são perdidas quando as SCPs são desabilitadas na organização. Se você quiser reabilitar as SCPs posteriormente, deverá anexá-las novamente à raiz, UOs e contas da organização, conforme apropriado.

**Permissões mínimas**

Para desativar as SCPs, você precisa de permissão para executar as seguintes ações:

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations
- `organizations:ListRoots` – necessário somente ao usar o console do Organizations

AWS Management Console

Para desabilitar um tipo de política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Policies (Políticas), escolha o nome do tipo de política que você deseja desabilitar.
3. Na página do tipo de política, escolha Desabilitar ***tipo de política***.
4. Na caixa de diálogo de confirmação, insira a palavra **`disable`**, depois, escolha Disable (Desabilitar).

   A lista de políticas disponíveis do tipo especificado desaparece.

AWS CLI & AWS SDKs

Para desabilitar um tipo de política

Você pode usar um dos seguintes comandos para desativar um tipo de política:

- AWS CLI: disable-policy-type

O exemplo a seguir mostra como desabilitar políticas de backup para sua organização. Observe que você deve especificar o ID da raiz da organização.

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
}
```

A lista de `PolicyTypes` na saída não inclui mais o tipo de política especificado.

- AWS SDKs: DisablePolicyType

# Obter informações sobre as políticas da sua organização

Esta seção descreve várias maneiras de obter detalhes sobre as políticas de sua organização. Estes procedimentos aplicam-se a todos os tipos de política. Você deve habilitar um tipo de política na raiz da organização antes de anexar políticas desse tipo a qualquer entidade na raiz da organização em questão.

## Listar todas as políticas

**Permissões mínimas**

Para listar as políticas da sua organização, você deve ter as seguintes permissões:

- `organizations:ListPolicies`

Você pode visualizar as políticas em sua organização no AWS Management Console ou usando um comando do AWS Command Line Interface (AWS CLI) ou uma operação do AWS SDK.

### AWS Management Console

Para listar todas as políticas de sua organização

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Policies (Políticas), escolha a política que deseja listar.

   Se o tipo de política especificado estiver habilitado, o console exibirá uma lista de todas as políticas desse tipo que estão atualmente disponíveis na organização.
3. Retorne à página Policies (Políticas) e repita para cada tipo de política.

### AWS CLI & AWS SDKs

Para listar todas as políticas de sua organização

Você pode usar um dos seguintes comandos para listar políticas em uma organização:

- AWS CLI: list-policies

  O exemplo a seguir mostra como obter uma lista de todas as políticas de controle de serviço de sua organização. Você deve especificar o tipo de política que deseja ver. Repita o comando para cada tipo de política que você deseja incluir.

```
$ aws organizations list-policies \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDKs: ListPolicies

## Listagem de todas as políticas anexadas a uma raiz, UO ou conta

**Permissões mínimas**

Para listar as políticas que são anexadas a uma raiz, unidade organizacional (UO) ou conta em sua organização, você deve ter as seguintes permissões:

- `organizations:ListPoliciesForTarget` com um elemento `Resource` na mesma instrução de política que inclui nome do recurso da Amazon (ARN) do alvo especificado (ou "*")

### AWS Management Console

Para listar todas as políticas que estão anexadas diretamente a uma raiz, UO ou conta especificada

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, escolha o nome da raiz, UO ou conta cujas políticas você deseja visualizar. Talvez seja necessário expandir as UOs (escolha ▶) para encontrar a conta que você deseja.
3. Na página Raiz, UO ou conta, escolha a guia Policies (Políticas).

   A guia Policies (Políticas) exibe todas as políticas anexadas a essa raiz, UO ou conta, agrupadas por tipo de política.

### AWS CLI & AWS SDKs

Para listar todas as políticas que estão anexadas diretamente a uma raiz, UO ou conta especificada

Você pode usar um dos seguintes comandos para listar políticas anexadas a uma entidade:

- AWS CLI: list-policies-for-target

  O exemplo a seguir lista todas as políticas de controle de serviço anexadas à UO especificada. Você deve especificar o ID da raiz, UO ou conta e o tipo de política que você deseja listar.

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDKs: ListPoliciesForTarget

## Listar todas as raízes, UOs e contas às quais uma política está anexada

> **Permissões mínimas**
>
> Para listar as entidades às quais uma política está anexada, você deve ter as seguintes permissões:
>
> - `organizations:ListTargetsForPolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política especificada (ou "*")

### AWS Management Console

Para listar todas as raízes, UOs e contas que têm uma política especificada anexada

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Policies (Políticas), escolha o tipo de política e, em seguida, escolha o nome da política cujos anexos você deseja examinar.
3. Selecione a guia Targets (Alvos) para exibir uma tabela de toda raiz, UO e conta à qual a política escolhida está anexada.

### AWS CLI & AWS SDKs

Para listar todas as raízes, UOs e contas que têm uma política especificada anexada

Você pode usar um dos seguintes comandos para entidades com uma política:

- AWS CLI: list-targets-for-policy

  O exemplo a seguir mostra todos os anexos à raiz, UOs e contas para a política especificada.

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
```

```
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- AWS SDKs: ListTargetsForPolicy

## Obter detalhes sobre uma política

> **Permissões mínimas**
>
> Para exibir os detalhes de uma política, você deve ter as seguintes permissões:
>
> - `organizations:DescribePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política especificada (ou "*")

AWS Management Console

Para obter detalhes sobre uma política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Policies (Políticas), escolha o tipo de política que você deseja examinar e, em seguida, escolha o nome da política.

   A página da política exibe as informações disponíveis sobre a política, incluindo seu ARN, descrição e anexos.

   - A guia Content (Conteúdo) mostra o conteúdo atual da política no formato JSON.

- A guia Targets (Alvos) mostra uma lista das raízes, UOs e contas às quais a política está anexada.
- A guia Tags mostra as tags anexadas à política. Observação: a guia Tags não está disponível para políticas gerenciadas pela AWS.

Para editar a política, escolha Editar política. Como cada tipo de política tem requisitos de edição diferentes, consulte as instruções para criar e atualizar políticas do tipo de política especificado.

AWS CLI & AWS SDKs

Para obter detalhes sobre uma política

Você pode usar um dos seguintes comandos para obter os detalhes sobre uma política:

- AWS CLI: describe-policy

  O exemplo a seguir exibe os detalhes da política especificada.

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*
\"\n    }\n  ]\n}"
    }
}
```

- AWS SDKs: DescribePolicy

# Administrador delegado para AWS Organizations

Recomendamos que você use a conta AWS Organizations de gerenciamento e seus usuários e funções somente para tarefas que devem ser executadas por essa conta. Também recomendamos armazenar todos os seus recursos da AWS em outras contas-membro na organização e mantê-las fora da conta de gerenciamento. Isso porque os recursos de segurança, como as políticas de controle de serviços (SCPs) do Organizations, não restringem usuários ou perfis na conta de gerenciamento.

Na conta de gerenciamento da organização, é possível delegar o gerenciamento de políticas do Organization para contas-membro especificadas para executar ações de políticas que, por padrão, estão disponíveis somente para a conta de gerenciamento.

## Criar ou atualizar uma política de delegação baseada em recursos

Na conta de gerenciamento, crie ou atualize uma política de delegação baseada em recursos para sua organização e adicione uma instrução que especifique quais contas-membro podem executar ações de acordo com as políticas. É possível adicionar diversas instruções na política para denotar um conjunto diferente de permissões às contas-membro.

Permissões mínimas

Para criar ou atualizar a política de delegação baseada em recursos, você precisa de permissões para executar as seguintes ações:

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

Além disso, você deve conceder aos perfis e usuários na conta do administrador delegado as permissões do IAM correspondentes para as ações necessárias. Sem as permissões do IAM, presume-se que o responsável pela chamada não tenha as permissões necessárias para gerenciar AWS Organizations políticas.

AWS Management Console

Adicione instruções à política de delegação baseada em recursos no AWS Management Console usando um dos métodos a seguir:

- Política JSON: cole e personalize um exemplo de política de delegação baseada em recursos para usar em sua conta ou digite seu próprio documento de política JSON no editor JSON.
- Editor visual: crie uma nova política de delegação no editor visual, que orienta você na criação de uma política de delegação sem a necessidade de escrever uma sintaxe JSON.

Usar o editor de políticas JSON para criar ou atualizar uma política de delegação

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Escolha Configurações.
3. Na seção Administrador delegado para o AWS Organizations, escolha Delegar para criar a política de delegação do Organizations. Para atualizar uma política de delegação existente, escolha Edit (Editar).
4. Digite ou cole um documento de política JSON. Para obter detalhes sobre a linguagem da política do IAM, consulte a referência de política JSON do IAM.
5. Resolva quaisquer avisos de segurança, erros ou avisos gerais gerados durante a validação da política e, em seguida, escolha Create policy (Criar política) para salvar seu trabalho.

Usar o editor visual para criar ou atualizar uma política de delegação

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Escolha Configurações.
3. Na seção Administrador delegado para o AWS Organizations, escolha Delegar para criar a política de delegação do Organizations. Para atualizar uma política de delegação existente, escolha Edit (Editar).
4. Na página Create Delegation policy (Criar política de delegação), escolha Add new statement (Adicionar nova instrução).
5. Defina Effect (Efeito) como `Allow`.
6. Adicione `Principal` para definir as contas-membro às quais você deseja delegar. Para obter detalhes sobre a sintaxe, consulte Exemplos de políticas de delegação baseadas em recursos.

7. Na lista de Actions (Ações), escolha as ações que deseja delegar. É possível usar Filter actions (Filtrar ações) para restringir as opções.
8. Para especificar se a conta-membro delegada pode anexar políticas à raiz da organização ou às unidades organizacionais (UOs), defina `Resources`. Você também deve selecionar `policy` como um tipo de recurso. Para obter detalhes adicionais, consulte as Exemplos de políticas de delegação baseadas em recursos. É possível especificar recursos das seguintes maneiras:

   - Escolha Add a resource (Adicionar um recurso) e crie o nome do recurso da Amazon (ARN) seguindo as instruções na caixa de diálogo.
   - Liste os ARNs dos recursos manualmente no editor. Para obter mais informações sobre a sintaxe do ARN, consulte Amazon Resource Name (ARN) no Guia de referência geral. AWS Para obter informações sobre como usar os ARNs no elemento de recurso de uma política, consulte Elementos de política JSON do IAM: Resource.
9. Escolha Add a condition (Adicionar uma condição) para especificar outras condições, incluindo o tipo de política que você deseja delegar. Escolha a Condition key (Chave de condição), a Tag key (Chave de etiqueta), o Qualifier (Qualificador) e o Operator (Operador) para a condição e, em seguida, digite um **`Value`**. Para obter detalhes adicionais, consulte Exemplos de políticas de delegação baseadas em recursos. Ao terminar, selecione Add condition (Adicionar condição). Para obter mais informações sobre o elemento Condition (Condição), consulte Elementos de política JSON do IAM: Condition na referência de política JSON do IAM.
10. Para adicionar mais blocos de permissão, escolha Add new statement (Adicionar nova instrução). Para cada bloco, repita as etapas de 5 a 9.
11. Resolva quaisquer avisos de segurança, erros ou avisos gerais gerados durante a validação da política e, em seguida, escolha Create policy (Criar política) para salvar seu trabalho.

AWS CLI & AWS SDKs

Criar ou atualizar uma política de delegação

É possível usar o comando a seguir para criar ou atualizar uma política de delegação:

- AWS CLI: put-resource-policy

  O exemplo a seguir cria ou atualiza uma política de delegação.

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            }
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

### Ações de política de delegação com suporte

Para a política de delegação, há suporte para as ações a seguir:

- `AttachPolicy`
- `CreatePolicy`
- `DeletePolicy`
- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `DetachPolicy`
- `DisablePolicyType`
- `EnablePolicyType`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`

- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`
- `TagResource`
- `UntagResource`
- `UpdatePolicy`

Teclas de condição suportadas

Somente as chaves de condição suportadas pelo AWS Organizations podem ser usadas para a política de delegação. Para obter mais informações, consulte Chaves de condição AWS Organizations na Referência de autorização de serviço.

## Visualizar uma política de delegação baseada em recursos

Na conta de gerenciamento, visualize a política de delegação baseada em recursos da sua organização para entender quais administradores delegados têm acesso para gerenciar quais tipos de política.

> **Permissões mínimas**
>
> Para visualizar a política de delegação baseada em recursos, você precisa de permissões para executar a seguinte ação: `organizations:DescribeResourcePolicy`.

AWS Management Console

Visualizar uma política de delegação

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Escolha Configurações.
3. Na seção Administrador delegado para o AWS Organizations, role para visualizar a política de delegação completa.

AWS CLI & AWS SDKs

Visualizar uma política de delegação

Você pode usar o comando a seguir para visualizar uma política de delegação:

- AWS CLI: describe-resource-policy

  O exemplo a seguir recupera a política.

  ```
  $ aws organizations describe-resource-policy
  ```

- AWS SDK: DescribeResourcePolicy

## Excluir uma política de delegação baseada em recursos

Quando não precisar mais delegar o gerenciamento de políticas em sua organização, você poderá excluir a política de delegação baseada em recursos da conta de gerenciamento da organização.

> **Important**
>
> Se você excluir sua política de delegação baseada em recursos, não será possível recuperá-la.

> **Permissões mínimas**
>
> Para excluir a política de delegação baseada em recursos, você precisa de permissões para executar a seguinte ação: `organizations:DeleteResourcePolicy`.

AWS Management Console

Excluir uma política de delegação

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

2. Escolha Configurações.
3. Na seção Administrador delegado para o AWS Organizations, escolha Excluir.
4. Na caixa de diálogo de confirmação para Delete policy (Excluir política), digite **`delete`**. Em seguida, escolha Delete policy (Excluir política).

AWS CLI & AWS SDKs

Excluir uma política de delegação

É possível usar o comando a seguir para excluir uma política de delegação:

- AWS CLI: delete-resource-policy

  O exemplo a seguir exclui a política.

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS SDK: DeleteResourcePolicy

## Exemplos de políticas de delegação baseadas em recursos

Os exemplos de código a seguir mostram como é possível usar políticas de delegação baseadas em recursos.

Exemplos

- Exemplo: visualizar organização, UOs, contas e políticas
- Exemplo: permissões consolidadas para gerenciar as políticas de backup de uma organização

### Exemplo: visualizar organização, UOs, contas e políticas

Antes de delegar o gerenciamento de políticas, você deve delegar as permissões para navegar na estrutura de uma organização e visualizar as unidades organizacionais (UOs), as contas e as políticas vinculadas a elas.

Este exemplo mostra como é possível incluir essas permissões na política de delegação baseada em recursos para a conta-membro, *`AccountId`*.

> **Important**
>
> É recomendável incluir permissões somente para as ações necessárias mínimas, conforme mostrado no exemplo, embora seja possível delegar qualquer ação somente leitura do Organizations usando esta política.

Este exemplo de política de delegação concede as permissões necessárias para concluir ações programaticamente da API AWS ou AWS CLI. Para usar esta política de delegação, substitua o texto do espaço reservado da AWS para *AccountId* com suas próprias informações. Em seguida, siga as instruções em Administrador delegado para AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

## Exemplo: permissões consolidadas para gerenciar as políticas de backup de uma organização

Este exemplo mostra como você pode criar uma política de delegação baseada em recursos que permite que a conta de gerenciamento delegue todas as permissões necessárias para gerenciar políticas de backup dentro da organização, incluindo as ações `create`, `read`, `update` e `delete`, bem como as ações da política `attach` e `detach`. Para compreender o significado de cada ação, recurso e condição, consulte Exemplos de políticas de delegação baseadas em recursos.

> **Important**
>
> Essa política permite que os administradores delegados executem as ações especificadas nas políticas criadas por qualquer conta na organização, incluindo a conta de gerenciamento.

Este exemplo de política de delegação concede as permissões necessárias para concluir ações programaticamente a partir da AWS API ou. AWS CLI Para usar essa política de delegação, substitua o texto AWS do espaço reservado para *`MemberAccountIdManagementAccountId`*, *`OrganizationId`*, e *`RootId`*por suas próprias informações. Em seguida, siga as instruções em Administrador delegado para AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
```

```
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

# Políticas de gerenciamento

As políticas de gerenciamento permitem configurar e gerenciar centralmente serviços da AWS e seus recursos. Como essas políticas afetam as UOs e as contas que as herdam depende do tipo de política de gerenciamento que você aplica no AWS Organizations. Revise os tópicos desta seção para compreender termos e conceitos relevantes sobre políticas de gerenciamento.

Tópicos



## Entendendo a herança da política de gerenciamento

> **Note**
>
> As informações nesta seção não se aplicam aos SCPs porque os SCPs gerenciam a permissão e a negação de ações do IAM. Embora os SCPs estejam vinculados à raiz, UOs e contas, permitir ações exige uma declaração `allow` explícita nos SCPs em todos os níveis, desde a raiz até cada UO no caminho direto para a conta (incluindo a própria conta de destino). Para obter mais informações sobre como os SCPs funcionam em uma hierarquia AWS Organizations, consulte Avaliação do SCP.

Você pode anexar políticas de gerenciamento a entidades da organização (raiz da organização, unidade organizacional (UO) ou conta) na sua organização:

- Quando você anexa uma política de gerenciamento à raiz da organização, todas as UOs e contas na organização herdam essa política.
- Quando você anexa uma política de gerenciamento a uma UO específica, as contas que estão diretamente sob essa UO ou qualquer UO filho herdam a política.
- Quando você anexa uma política de gerenciamento a uma conta específica, ela afeta apenas essa conta.

Como você pode anexar políticas de gerenciamento a vários níveis na organização, as contas podem herdar várias políticas.

Esta seção explica como as políticas pai e as políticas filho são processadas na política efetiva de uma conta.

Tópicos



## Terminologia de herança

Este tópico usa os seguintes termos ao discutir herança de política de gerenciamento.

Herança de política

A interação de políticas em diferentes níveis de uma organização se move da raiz de nível superior da organização passando pela hierarquia de unidade organizacional (UO) para contas individuais.

Você pode anexar políticas à raiz da organização, UOs, contas individuais e a qualquer combinação dessas entidades da organização. Herança de política de gerenciamento se refere a políticas anexadas à raiz da organização ou a uma UO. Todas as contas que são membros da raiz da organização ou UO em que uma política de gerenciamento está anexada herdam essa política.

Por exemplo, quando as políticas de gerenciamento são anexadas à raiz da organização, todas as contas na organização herdam essa política. Isso ocorre porque todas as contas em uma organização estão sempre sob a raiz da organização. Quando você anexa uma política a uma UO específica, as contas que estão diretamente sob essa UO ou qualquer UO filho herdam essa política. Como você pode anexar políticas a vários níveis na organização, as contas podem herdar vários documentos de política para um único tipo de política.

Políticas principais

As políticas anexadas em um nível superior na árvore organizacional em relação à políticas anexadas a entidades inferiores na árvore.

Por exemplo, se você anexar a política de gerenciamento A à raiz da organização, ela será apenas uma política. Se também anexar a política B a uma UO nessa raiz, a política A será a política pai da política B. A política B será a política filho da política A. As políticas A e B serão mescladas para criar a política de tag efetiva para contas na UO.

Políticas secundárias

As políticas anexadas em um nível inferior na árvore organizacional em relação à política pai.

Políticas efetivas

Um documento de política único e definitivo que especifica as regras de atribuição que se aplicam a uma conta. A política efetiva é a agregação de todas as políticas herdadas pela conta, além de qualquer política diretamente anexada à conta. Por exemplo, as políticas de tag permitem que você exiba a política de tag efetiva que se aplica a qualquer uma de suas contas. Para obter mais informações, consulte Visualizar políticas de tag efetivas.

Operadores de herança

Operadores que controlam como as políticas herdadas se mesclam em uma única política efetiva. Esses operadores são considerados um recurso avançado. Os autores experientes de política podem usá-los para limitar as alterações que uma política filho pode fazer e como as configurações nas políticas são mescladas. Para obter mais informações, consulte Operadores de herança.

## Sintaxe de política e herança para tipos de política de gerenciamento

Exatamente como as políticas de gerenciamento afetarão as UOs e as contas que as herdam dependerá do tipo de política que você escolher. Os tipos de políticas de gerenciamento incluem:

- Políticas de exclusão de serviços de inteligência artificial (IA)
- Políticas de backup
- Políticas de tag

A sintaxe de tipos de política de gerenciamento inclui Operadores de herança, que permitem especificar com granularidade fina quais elementos das políticas superiores são aplicados e quais elementos podem ser substituídos ou modificados por UOs e contas subordinadas.

A política efetiva é o conjunto de regras que são herdadas da raiz da organização e das UOs, juntamente com as diretamente anexadas à conta. A política em vigor especifica as regras que se

aplicam à conta. É possível visualizar a política efetiva para uma conta que inclui o efeito de todos os operadores de herança nas políticas aplicadas. Para obter mais informações, consulte Visualizar políticas de tag efetivas.

## Operadores de herança

Operadores de herança controlam como as políticas herdadas e as políticas de conta se fundem na política efetiva da conta. Esses operadores incluem operadores de definição de valor e operadores de controle filho.

Quando você usa o editor visual no console do AWS Organizations, você pode usar apenas o operador `@@assign`. Outros operadores são considerados um recurso avançado. Para usar os outros operadores, você deve criar manualmente a política JSON. Os autores experientes de política podem usar os operadores de herança para controlar quais valores são aplicados à política efetiva e limitar as alterações que as políticas filho podem fazer.

Operadores de definição de valor

Você pode usar os seguintes operadores de definição de valor para controlar como a política interage com suas políticas pai:

- `@@assign` – Substitui quaisquer configurações de política herdadas pelas configurações especificadas. Se a configuração especificada não for herdada, esse operador a adicionará à política efetiva. Esse operador pode se aplicar a qualquer configuração de política de qualquer tipo.
  - Para configurações de valor único, esse operador substitui o valor herdado pelo valor especificado.
  - Para configurações de valores múltiplos (matrizes JSON), esse operador remove quaisquer valores herdados e os substitui pelos valores especificados por esta política.
- `@@append` – Adiciona as configurações especificadas às herdadas (sem remover nenhuma). Se a configuração especificada não for herdada, esse operador a adicionará à política efetiva. Você pode usar esse operador apenas com configurações de vários valores.
  - Este operador adiciona os valores especificados a quaisquer valores na matriz herdada.
- `@@remove` – Remove as configurações herdadas especificadas da política em vigor, se houver. Você pode usar esse operador apenas com configurações de vários valores.
  - Esse operador remove somente os valores especificados da matriz de valores herdados das políticas pai. Outros valores podem continuar a existir na matriz e podem ser herdados por políticas filho.

### Operadores de controle filho

O uso de operadores de controle filho é opcional. Você pode usar o operador `@@operators_allowed_for_child_policies` para controlar quais operadores de definição de valor as políticas filho podem usar. Você pode permitir todos os operadores, alguns operadores específicos ou nenhum operador. Por padrão, todos os operadores (`@@all`) são permitidos.

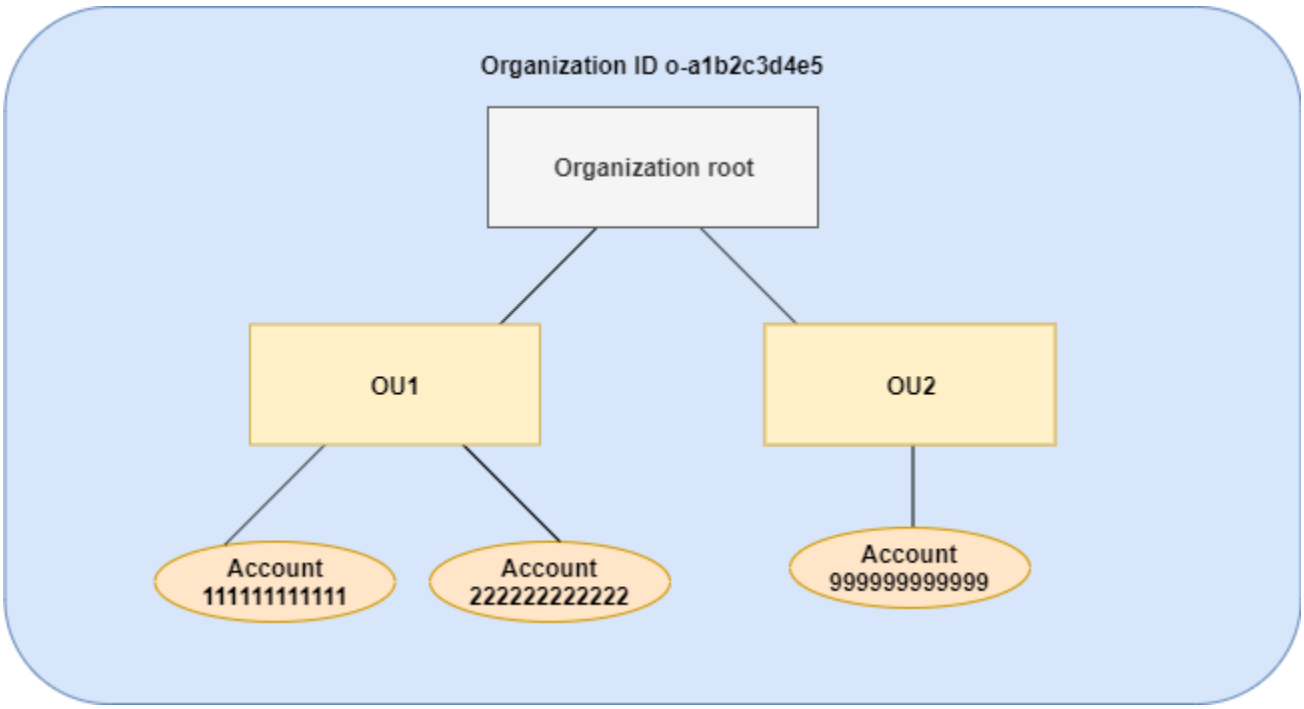
- `"@@operators_allowed_for_child_policies":["@@all"]` – UOs e contas subordinadas podem usar qualquer operador em políticas. Por padrão, todos os operadores são permitidos em políticas filho.
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` – Contas e UOs subordinadas podem usar somente os operadores especificados em políticas subordinadas. Você pode especificar um ou mais operadores de definição de valor neste operador de controle filho.
- `"@@operators_allowed_for_child_policies":["@@none"]` – UOs e contas subordinadas não podem usar operadores em políticas. Você pode usar este operador para bloquear efetivamente valores definidos em uma política pai de modo que as políticas filho não possam adicionar, acrescentar ou remover tais valores.

> **Note**
>
> Se um operador de controle filho herdado limitar o uso de um operador, você não poderá reverter essa regra em uma política filho. Se você incluir operadores de controle filho em uma política pai, eles limitarão os operadores de definição de valor em todas as políticas filho.

## Exemplos de herança

Estes exemplos mostram como a herança de política funciona ao exibir como as políticas de tag pai e filho são mescladas em uma política de tag efetiva para uma conta.

Os exemplos assumem que você tem a estrutura de organização exibida no diagrama a seguir.




Exemplos

- Exemplo 1: permitir que políticas filho substituam apenas valores de tag
- Exemplo 2: anexar novos valores a tags herdadas
- Exemplo 3: remover valores de tags herdadas
- Exemplo 4: restringir alterações às políticas filho
- Exemplo 5: conflitos com operadores de controle filho
- Exemplo 6: conflitos com a anexação de valores no mesmo nível de hierarquia

Exemplo 1: permitir que políticas filho substituam apenas valores de tag

A política de tags a seguir define a chave de tag `CostCenter` e dois valores aceitáveis, `Development` e `Support`. Se você anexá-la à raiz da organização, a política de tag estará em vigor para todas as contas na organização.

Política A — Política de tag da raiz da organização

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
```

```
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Vamos supor que você deseje que os usuários na UO1 usem um valor de tag diferente para uma chave. Além disso, você deseja aplicar a política de tag a tipos de recursos específicos. Como a política A não especifica quais operadores de controle filho são permitidos, todos os operadores são permitidos. Você pode usar o operador `@@assign` e criar uma política de tag como a seguinte para anexar à UO1.

Política B — Política de tag da UO1

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Isto é o que acontece ao especificar o operador `@@assign` para a tag quando a política A e a política B são mescladas para formar a política de tag efetiva para uma conta:

- A política B substitui os dois valores de tag que foram especificados na política pai, a política A. O resultado é que `Sandbox` é apenas o valor compatível para a chave de tag `CostCenter`.
- A adição de `enforced_for` especifica que a tag `CostCenter` deve ser o valor de tag especificado em todos os recursos do Amazon RedShift e tabelas do Amazon DynamoDB.

Como mostrado no diagrama, a UO1 inclui duas contas: 111111111111 e 222222222222.

Política de tags efetiva resultante para contas 111111111111 e 222222222222

> **Note**
>
> Você não pode usar diretamente o conteúdo de uma política em vigor exibida como o conteúdo de uma nova política. A sintaxe não inclui os operadores necessários para controlar a mesclagem com outras políticas superiores e subordinadas. A exibição de uma política em vigor destina-se apenas à compreensão dos resultados da fusão.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Exemplo 2: anexar novos valores a tags herdadas

Pode haver casos em que você deseja que todas as contas da organização especifiquem uma chave de tag com uma pequena lista de valores aceitáveis. Para contas em uma UO, convém permitir um valor adicional que somente essas contas possam especificar ao criar recursos. Este exemplo especifica como fazer isso usando o operador `@@append`. O operador `@@append` é um recurso avançado.

Como o exemplo 1, este exemplo começa com a política A para a política de tag da raiz da organização.

Política A — Política de tag da raiz da organização

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Para este exemplo, anexe a política C à UO2. A diferença neste exemplo é que o uso do operador `@@append` na política C adiciona, em vez de substituir, a lista de valores aceitáveis e a regra `enforced_for`.

Política C — Política de tag da UO2 para valores anexos

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
```

```
            }
        }
    }
}
```

Anexar a política C à UO2 tem os seguintes efeitos quando a política A e a política C são mescladas para formar a política de tags efetiva para uma conta:

- Como a política C inclui o operador `@@append`, ela permite adicionar, e não substituir, a lista de valores de tag aceitáveis especificados na Política A.
- Como na política B, a adição de `enforced_for` especifica que a tag `CostCenter` deve ser usada como valor de tag especificado em todos os recursos do Amazon RedShift e tabelas do Amazon DynamoDB. Substituir (`@@assign`) e adicionar (`@@append`) terão o mesmo efeito se a política pai não incluir um operador de controle filho que restrinja o que uma política filho pode especificar.

Como mostrado no diagrama, a UO2 inclui uma conta: 999999999999. A política A e a política C são mescladas para criar a política de tag efetiva para a conta 999999999999.

Política de tag efetiva para a conta 999999999999

> **Note**
>
> Você não pode usar diretamente o conteúdo de uma política em vigor exibida como o conteúdo de uma nova política. A sintaxe não inclui os operadores necessários para controlar a mesclagem com outras políticas superiores e subordinadas. A exibição de uma política em vigor destina-se apenas à compreensão dos resultados da fusão.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
                "Support",
                "Marketing"
            ],
            "enforced_for": [
```

```
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Exemplo 3: remover valores de tags herdadas

Pode haver casos em que a política de tag anexada à organização defina mais valores de tag do que aqueles você deseja que uma conta use. Este exemplo explica como revisar uma política de tag usando o operador `@@remove`. O `@@remove` é um recurso avançado.

Como os outros exemplos, este exemplo começa com a política A para a política de tag da raiz da organização.

Política A — Política de tag da raiz da organização

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Para este exemplo, anexe a política D à conta 999999999999.

Política D — Política de tag da conta 999999999999 para remoção de valores

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
```

```
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

A anexação da política D à conta 999999999999 tem os efeitos a seguir quando as políticas A, C e D se mesclam para formar a política de tags efetiva:

- Supondo que você executou todos os exemplos anteriores, as políticas B, C e C são políticas filho da A. A política B é anexada somente à UO1, portanto não tem efeito na conta 9999999999999.
- Para a conta 9999999999999, o único valor aceitável para a chave de tag `CostCenter` é `Support`.
- A conformidade não é imposta para a chave de tag `CostCenter`.

Nova política de tag eficaz para a conta 999999999999

> **Note**
>
> Você não pode usar diretamente o conteúdo de uma política em vigor exibida como o conteúdo de uma nova política. A sintaxe não inclui os operadores necessários para controlar a mesclagem com outras políticas superiores e subordinadas. A exibição de uma política em vigor destina-se apenas à compreensão dos resultados da fusão.

```
{
    "tags": {
        "costcenter": {
```

```
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

Se posteriormente você adicionar mais contas à UO2, as políticas de tag efetivas serão diferentes das da conta 999999999999. Isso ocorre porque a política mais restritiva D é anexada apenas no nível da conta, e não à UO.

Exemplo 4: restringir alterações às políticas filho

Pode haver casos em que você queira restringir as alterações nas políticas filho. Este exemplo explica como fazer isso usando operadores de controle filho.

Este exemplo começa com uma nova política de tag da raiz da organização e assume que as políticas de tag ainda não estão anexadas a entidades da organização.

Política E: política de tag da raiz da organização para restringir alterações em políticas subordinadas

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

Quando você anexa a política E à raiz da organização, ela impede que as políticas filho alterem a chave de tag `Project`. No entanto, as políticas filho podem substituir ou anexar valores de tag.

Vamos supor que depois você anexe a seguinte política F a uma UO.

Política F — Política de tag da UO

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

Mesclar as políticas E e F tem os seguintes efeitos nas contas da UO:

- A política F é uma política filho da Política E.
- A política F tenta mudar o tratamento do caso, apesar de não ser possível. Isso ocorre porque a política E inclui o operador `"@@operators_allowed_for_child_policies": ["@@none"]` para a chave de tag.
- No entanto, a política F pode anexar valores de tag para a chave. Isso ocorre porque a política E inclui `"@@operators_allowed_for_child_policies": ["@@append"]` para o valor da tag.

Política efetiva para contas na UO

> **Note**
>
> Você não pode usar diretamente o conteúdo de uma política em vigor exibida como o conteúdo de uma nova política. A sintaxe não inclui os operadores necessários para controlar a mesclagem com outras políticas superiores e subordinadas. A exibição de uma política em vigor destina-se apenas à compreensão dos resultados da fusão.

```
{
```

```
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
        }
    }
}
```

Exemplo 5: conflitos com operadores de controle filho

Os operadores de controle filho podem existir em políticas de tag anexadas no mesmo nível na hierarquia da organização. Quando isso acontece, a interseção dos operadores permitidos é usada quando as políticas se mesclam para formar a política efetiva das contas.

Suponha que as políticas G e H estão anexadas à raiz da organização.

Política G — Política de tag da raiz da organização 1

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

Política H — Política de tag da raiz da organização 2

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
```

```
            }
        }
    }
}
```

Neste exemplo, uma política na raiz da organização define que os valores da chave de tag só podem ser anexados. A outra política anexada à raiz da organização permite que as políticas filho anexem e removam valores. A interseção dessas duas permissões é usada para políticas filho. O resultado é que as políticas filho podem anexar valores, mas não remover valores. Portanto, a política filho pode anexar um valor à lista de valores de tag, mas não pode remover o valor `Maintenance`.

Exemplo 6: conflitos com a anexação de valores no mesmo nível de hierarquia

Você pode anexar várias políticas de tag a cada entidade da organização. Quando você fizer isso, as políticas de tag anexadas à mesma entidade da organização podem incluir informações conflitantes. As políticas são avaliadas com base na ordem em que foram anexadas à entidade da organização. Para alterar qual política é avaliada primeiro, você pode desanexar uma política e reanexá-la.

Suponha que a política J tenha sido a primeira a ser anexada à raiz da organização, e a política K tenha sido a segunda.

Política J — Primeira política de tag anexada à raiz da organização

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

Política K — Segunda política de tag anexada à raiz da organização

```
{
    "tags": {
        "project": {
```

```
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

Neste exemplo, a chave de tag PROJECT é usada na política de tag efetiva porque a política que a definiu foi anexada à raiz da organização primeiro.

Política JK — Política de tag em vigor para a conta

A política efetiva para a conta é a seguinte.

> **Note**
>
> Você não pode usar diretamente o conteúdo de uma política em vigor exibida como o conteúdo de uma nova política. A sintaxe não inclui os operadores necessários para controlar a mesclagem com outras políticas superiores e subordinadas. A exibição de uma política em vigor destina-se apenas à compreensão dos resultados da fusão.

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

## Políticas de exclusão dos serviços de IA

Os serviços de inteligência artificial (IA) da AWS, entre eles, Amazon Rekognition, Amazon CodeWhisperer, Amazon Transcribe e Contact Lens for Amazon Connect, podem armazenar e usar o conteúdo dos clientes processado por esses serviços para promover o desenvolvimento e a melhoria contínua de outros serviços da AWS. Como um cliente da AWS, você pode optar por não ter o seu conteúdo armazenado nem utilizado para melhorias no serviço.

> **Note**
>
> Talvez os serviços de inteligência artificial (IA) da AWS precisem armazenar seus dados mesmo se você não permitir que a AWS use seus dados para realizar melhorias no serviço. Para obter mais informações, consulte a documentação do serviço de IA que está usando.

Em vez de definir essa configuração individualmente para cada Conta da AWS que sua organização usa, você pode configurar uma política de organização que aplique sua escolha de configuração a todas as contas que são membros da organização. Você pode optar por não ter conteúdo armazenado e utilizado para um serviço de IA individual ou para todos os serviços cobertos de uma só vez. Você pode consultar a política aplicável em vigor para cada conta para ver os efeitos de suas escolhas de configuração.

> **Important**
>
> - Quando você especifica uma preferência de optar ou não optar para um serviço, essa configuração é global e aplicada a todas as Regiões da AWS. A configuração do valor de dentro de uma Região da AWS é replicada para todas as outras regiões.
> - Quando você opta por não usar conteúdo por um serviço de IA da AWS, esse serviço exclui todo o conteúdo histórico associado que foi compartilhado com a AWS antes de você definir a opção. Essa exclusão deve ser limitada a dados armazenados que não são necessários para fornecer funções de serviço.

## Introdução às políticas de exclusão dos serviços de IA

Siga estas etapas para começar a usar as políticas de exclusão dos serviços de inteligência artificial (IA).

1. Habilitar políticas de exclusão dos serviços de IA para sua organização.
2. Criar uma política de exclusão dos serviços de IA.
3. Anexe a política de exclusão dos serviços de IA à raiz, UO ou conta da sua organização.
4. Visualize a política combinada de exclusão dos serviços de IA em vigor que se aplica a uma conta.

Para todas essas etapas, você deve fazer login como usuário do AWS Identity and Access Management (IAM), assumir uma função do IAM, ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

Outras informações

- Aprenda a sintaxe de política para as políticas de exclusão dos serviços de IA e veja exemplos de política

## Criação, atualização e exclusão de políticas de exclusão dos serviços de IA

Neste tópico:

- Depois de habilitar as políticas de exclusão dos serviços de IA para sua organização, você pode criar uma política.
- Quando os requisitos de exclusão forem alterados, você poderá atualizar uma política existente.
- Quando você não precisar mais de uma política e depois de desvinculá-la de todas as unidades organizacionais (UOs) e contas, você poderá excluí-la.

### Criação de uma política de exclusão dos serviços de IA

> **Permissões mínimas**
>
> Para criar uma política de exclusão dos serviços de IA, você precisa de permissão para executar a seguinte ação:
>
> - `organizations:CreatePolicy`

#### AWS Management Console

Para criar uma política de exclusão dos serviços de IA

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página AI services opt-out policies (Políticas de exclusão dos serviços de IA), escolha Create policy (Criar política).

3. Na página Create new AI services opt-out policy (Criar nova política de exclusão dos serviços de IA), insira um nome da política e uma descrição da política, opcional.
4. (Opcional) você pode adicionar uma ou mais tags escolhendo Add tag (Adicionar tag) e inserindo uma chave e um valor opcional. Se deixar o valor em branco, ele é definido como uma sequência vazia, não `null`. É possível anexar até 50 tags a uma política. Para mais informações, consulte Marcando atributos AWS Organizations.
5. Insira ou cole o texto da política na guia JSON. Para obter informações sobre a sintaxe das políticas de exclusão dos serviços de IA, consulte Sintaxe e exemplos de política de exclusão dos serviços de IA. Para obter exemplos de política que você pode usar como ponto de partida, consulte Exemplos de política de exclusão dos serviços de IA.
6. Quando terminar de editar sua política, escolha Create policy (Criar política) no canto inferior direito da página.

AWS CLI & AWS SDKs

Para criar uma política de exclusão dos serviços de IA

Você pode usar um dos seguintes procedimentos para criar uma política de tags:

- AWS CLI: create-policy

1. Crie uma política de exclusão dos serviços de IA como a seguinte e armazene-a em um arquivo de texto. Observe que "`optOut`" e "`optIn`" diferenciam entre maiúsculas e minúsculas.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Esta política de exclusão dos serviços de IA especifica que todas as contas afetadas pela política sejam excluídas de todos os serviços de IA, exceto o Amazon Rekognition.

2. Importe o arquivo de política JSON para criar uma nova política na organização. Neste exemplo, o arquivo JSON anterior foi chamado de `policy.json`.

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWS SDKs: CreatePolicy

O que fazer em seguida

Depois de criar uma política de exclusão dos serviços de IA, você pode colocar suas opções de exclusão em vigor. Para isso, você pode anexar a política à raiz da organização, unidades organizacionais (UOs), Contas da AWS dentro da organização ou uma combinação de tudo isso.

Atualização de uma política de exclusão dos serviços de IA

> **Permissões mínimas**
>
> Para atualizar uma política de exclusão dos serviços de IA, você deve ter permissão para executar as seguintes ações:

- `organizations:UpdatePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política especificada (ou "*")
- `organizations:DescribePolicy` com um elemento `Resource` na mesma instrução de política que inclui nome do recurso da Amazon (ARN) da política especificada (ou "*")

AWS Management Console

Para atualizar uma política de exclusão dos serviços de IA

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página AI services opt-out policies (Políticas de exclusão dos serviços de IA), escolha o nome da política que você deseja atualizar.
3. Na página de detalhes da política, escolha Edit policy (Editar política).
4. Você pode inserir um novo nome de política,descrição de política ou editar o texto de política JSON. Para obter informações sobre a sintaxe das políticas de exclusão dos serviços de IA, consulte Sintaxe e exemplos de política de exclusão dos serviços de IA. Para obter exemplos de política que você pode usar como ponto de partida, consulte Exemplos de política de exclusão dos serviços de IA.
5. Quando terminar de atualizar a política, escolha Salvar alterações.

AWS CLI & AWS SDKs

Para atualizar uma política

Você pode usar uma das seguintes opções para atualizar uma política:

- AWS CLI: update-policy

  O exemplo a seguir renomeia uma política de exclusão dos serviços de IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

O exemplo a seguir adiciona ou altera a descrição de uma política de exclusão dos serviços de IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

O exemplo a seguir altera o documento de política JSON anexado a uma política de exclusão dos serviços de IA. Neste exemplo, o conteúdo é retirado de um arquivo chamado `policy.json` com o seguinte texto:

```
{
    "services": {
        "default": {
```

```
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n}\n"}
}
```

- AWS SDKs: UpdatePolicy

### Edição de tags anexadas a uma política de exclusão dos serviços de IA

Quando faz login na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a uma política de exclusão dos serviços de IA. Para obter mais informações sobre marcação, consulte Marcando atributos AWS Organizations.

**Permissões mínimas**

Para editar as tags anexadas a uma política de exclusão dos serviços de IA em sua organização da AWS, você deve ter as seguintes permissões:

- `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations
- `organizations:DescribePolicy` – necessário somente ao usar o console do Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

#### AWS Management Console

Para editar as tags anexadas a uma política de exclusão dos serviços de IA

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página AI services opt-out policies (Políticas de exclusão dos serviços de IA), escolha o nome da política que você deseja editar.
3. Na página de detalhes da política, escolha a guia Tags, depois escolha Manage tags (Gerenciar tags).
4. Você pode executar qualquer uma das seguintes ações nesta página:
   - Edite o valor de qualquer tag inserindo um novo valor sobre o antigo. Não é possível modificar a chave. Para alterar uma chave, você deve excluir a tag com a chave antiga e adicionar uma tag com a nova chave.
   - Remova uma tag existente escolhendo Remove (Remover).

- Adicione um novo par de chave e valor de tag. Escolha Add tag (Adicionar tag) e insira o novo nome da chave e o valor opcional nas caixas fornecidas. Se você deixar a caixa Value (Valor) vazia, o valor é uma sequência vazia, não é `null`.

5. Escolha Save changes (Salvar alterações) depois de ter feito todas as adições, remoções e edições que deseja fazer.

AWS CLI & AWS SDKs

Para editar as tags anexadas a uma política de exclusão dos serviços de IA

Você pode usar um dos seguintes comandos para editar as tags anexadas a uma política de exclusão dos serviços de IA:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Exclusão de uma política de exclusão dos serviços de IA

Quando faz login na conta de gerenciamento da sua organização, você pode excluir uma política que não seja mais necessária em sua organização.

Antes de excluir uma política, você deve primeiro desvinculá-la de todas as entidades anexadas.

Permissões mínimas

Para excluir uma política, você deve ter permissão para executar a seguinte ação:

- `organizations:DescribePolicy` (somente console – para navegar até a política)
- `organizations:DeletePolicy`

AWS Management Console

Para excluir uma política de exclusão dos serviços de IA

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

2. Na página AI services opt-out policies (Políticas de exclusão dos serviços de IA), escolha o nome da política que você deseja excluir.
3. Você primeiro deve desvincular a política que deseja excluir de todas as raízes, UOs e contas. Escolha a guia Targets (Alvos), escolha o botão de opção ao lado de cada raiz, UO ou conta que é mostrada na lista Targets (Alvos) e escolha Detach (Desvincular). Na caixa de diálogo de confirmação, escolha Detach (Desvincular). Repita até remover todos os alvos.
4. Escolha Delete (Excluir), no alto da página.
5. Na caixa de diálogo de confirmação, insira o nome da política e escolha Delete (Excluir).

AWS CLI & AWS SDKs

Para excluir uma política de exclusão dos serviços de IA

Você pode usar uma das seguintes opções para excluir uma política:

- AWS CLI: delete-policy

  O exemplo a seguir exclui a política especificada. Ele só funciona se a política não estiver anexada a nenhuma raiz, UO ou conta.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: DeletePolicy

## Anexação e desvinculação de políticas de exclusão dos serviços de IA

Você pode usar políticas de exclusão de serviços de inteligência artificial (IA) em uma organização inteira, bem como em unidades organizacionais (UOs) e contas individuais. A que a política de exclusão dos serviços de IA se aplica depende do elemento de organização ao qual você a anexa:

- Quando você anexa uma política de exclusão dos serviços de IA à raiz da organização, a política se aplica a todas as UOs e contas-membro dessa raiz.
- Quando você anexa uma política de exclusão dos serviços de IA a uma UO, essa política se aplica às contas que pertencem à UO ou às suas UO subordinadas. Essas contas também estão sujeitas a qualquer política anexada à raiz da organização.

- Quando você anexa uma política de exclusão dos serviços de IA a uma conta, essa política se aplica somente a essa conta. A conta também está sujeita a qualquer política anexada à raiz da organização e a qualquer UO a que a conta pertence.

A agregação de todas as políticas de exclusão dos serviços de IA que a conta herda da raiz e das UOs superiores, bem como todas as políticas diretamente anexadas à conta, é a política em vigor. Para obter informações sobre como as políticas são mescladas à política efetiva, consulte Entendendo a herança da política de gerenciamento.

> **Permissões mínimas**
>
> Para anexar as políticas de exclusão dos serviços de IA, você deve ter permissão para executar a seguintes ação:
>
> - `organizations:AttachPolicy`

AWS Management Console

Você pode anexar uma política de exclusão dos serviços de IA navegando até a política ou até a raiz, UO ou conta à qual você deseja anexar a política.

Para anexar uma política de exclusão dos serviços de IA navegando até a raiz, UO ou conta

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue e escolha o nome da raiz, UO ou conta à qual você deseja anexar a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
3. Na guia Policies (Políticas), na entrada para Políticas de exclusão de serviço de IA, escolha Attach (Anexar).
4. Encontre a política que você deseja e escolha Attach policy (Anexar política).

   A lista de políticas de exclusão dos serviços de IA anexadas na guia Policies (Políticas) é atualizada para incluir a nova adição. A política entra em vigor imediatamente.

Para anexar uma política de exclusão dos serviços de IA navegando até a política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página AI services opt-out policies (Políticas de exclusão dos serviços de IA), escolha o nome da política que você deseja anexar.
3. Na guia Targets (Alvos), selecione Attach (Anexar).
4. Escolha o botão de opção ao lado da raiz, UO ou conta à qual você deseja anexar a política. Talvez seja necessário expandir as UOs (escolha ) para encontrar a UO ou a conta que você deseja.
5. Escolha Attach policy (Anexar política).

   A lista de políticas de exclusão dos serviços de IA anexadas na guia Targets (Alvos) é atualizada para incluir a nova adição. A política entra em vigor imediatamente.

AWS CLI & AWS SDKs

Para anexar a política de exclusão dos serviços de IA à raiz, UO ou conta da sua organização

Você pode usar um dos seguintes procedimentos para anexar uma política de exclusão dos serviços de IA:

- AWS CLI: attach-policy

  O exemplo a seguir anexa uma política a um principal.

  ```
  $ aws organizations attach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: AttachPolicy

A política entra em vigor imediatamente.

## Desvinculação de uma política de exclusão dos serviços de IA

Quando faz login na conta de gerenciamento da organização, você pode desvincular a política de exclusão dos serviços de IA da raiz, UO ou conta da organização à qual ela está anexada. Depois que você desvincular uma política de exclusão dos serviços de IA uma entidade, essa política não será mais aplicada a nenhuma conta afetada anteriormente pela entidade agora desvinculada. Para separar uma política, conclua as seguintes etapas.

> **Permissões mínimas**
>
> Para desvincular uma política de exclusão dos serviços de IA da raiz da organização, UO ou conta, você deve ter permissão para executar a seguinte ação:
>
> - `organizations:DetachPolicy`

### AWS Management Console

Você pode desvincular uma política de exclusão dos serviços de IA navegando até a política ou até a raiz, UO ou conta da qual você deseja desvincular a política.

Para desvincular uma política de exclusão dos serviços de IA navegando até a raiz, UO ou conta à qual ela está anexada

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue até a raiz, UO ou conta da qual você deseja desvincular uma política. Talvez seja necessário expandir as UOs (escolha ▶) para encontrar a UO ou a conta que você deseja. Escolha o nome da raiz, UO ou conta.
3. Na guia Policies (Políticas), escolha o botão de opção ao lado da política de exclusão dos serviços de IA que você deseja desvincular e selecione Desvincular.
4. Na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

   A lista de políticas de exclusão dos serviços de IA anexadas é atualizada. A política entra em vigor imediatamente.

Para desvincular uma política de exclusão dos serviços de IA navegando até a política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página AI services opt-out policies (Políticas de exclusão dos serviços de IA), escolha o nome da política que você deseja desvincular de uma raiz, UO ou conta.
3. Na guia Targets (Alvos), escolha o botão de opção ao lado da raiz, UO ou conta da qual você deseja desvincular a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
4. Escolha Detach (Desvincular).
5. Na caixa de diálogo de confirmação, escolha Detach (Desvincular).

   A lista de políticas de exclusão dos serviços de IA anexadas é atualizada. A política entra em vigor imediatamente.

AWS CLI & AWS SDKs

Para desvincular a política de exclusão dos serviços de IA da raiz, UO ou conta da sua organização

Você pode usar um dos seguintes comandos para desvincular uma política de exclusão dos serviços de IA:

- AWS CLI: detach-policy

  O exemplo a seguir desvincula uma política de uma UO.

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: DetachPolicy

A política entra em vigor imediatamente.

## Visualização de políticas de exclusão dos serviços de IA em vigor

Determine a política de exclusão de serviços de Inteligência Artificial (IA) de uma conta na sua organização.

Qual é a política de exclusão dos serviços de IA em vigor?

A política de exclusão dos serviços de IA em vigor especifica as regras finais que se aplicam a uma Conta da AWS. É a agregação de todas as políticas de exclusão dos serviços de IA que a conta herda, além de todas as políticas de exclusão dos serviços de IA diretamente anexada à conta. Quando você anexa uma política de exclusão dos serviços de IA à raiz da organização, ela se aplica a todas as contas na organização. Quando você anexa uma política de exclusão dos serviços de IA a uma UO, ela se aplica a todas as contas e UOs que pertencem à UO. Quando você anexa uma política diretamente a uma conta, ela se aplica somente a essa uma Conta da AWS.

Por exemplo, a política de exclusão dos serviços de IA anexada à raiz da organização pode especificar que todas as contas na organização optam por não ter seu conteúdo usado por nenhum dos serviços de machine learning da AWS. Uma política de exclusão dos serviços de IA separada, anexada diretamente a uma conta-membro especifica que opta por ter seu conteúdo usado apenas para o Amazon Rekognition. A combinação dessas políticas de exclusão dos serviços de IA constitui a política de exclusão dos serviços de IA em vigor. O resultado é que todas as contas na organização excluem todos os serviços da AWS, com exceção de uma conta que opta a incluir o Amazon Rekognition.

Para obter informações sobre como as políticas de exclusão dos serviços de IA são combinadas na política final em vigor, consulte Entendendo a herança da política de gerenciamento.

Saiba como visualizar a política de exclusão dos serviços de IA em vigor

Você pode visualizar a política de exclusão dos serviços de IA em vigor para uma conta no AWS Management Console, na API da AWS ou no AWS Command Line Interface.

**Permissões mínimas**

Para visualizar a política de exclusão dos serviços de IA em vigor para uma conta, você deve ter permissão para executar as seguintes ações:

- `organizations:DescribeEffectivePolicy`

- `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations

### AWS Management Console

Para visualizar a política de exclusão dos serviços de IA em vigor para uma conta

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, escolha o nome da conta para a qual você deseja visualizar a política de exclusão dos serviços de IA em vigor. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a conta que você deseja.
3. Na guia Policies (Políticas), na seção AI services opt-out policies (Políticas de cancelamento de serviços de IA), escolha View the effective IA policy for this Conta da AWS (Visualizar a política de exclusão dos serviços de IA em vigor para esta ).

   O console exibe a política em vigor aplicada à conta especificada.

   > **Note**
   >
   > Não é possível copiar e colar uma política de exclusão dos serviços de IA e usá-la como JSON para outra política de exclusão dos serviços de IA sem alterações significativas. Documentos de política de exclusão dos serviços de IA devem incluir os operadores de herança que especificam como cada configuração é mesclada na política final em vigor.

### AWS CLI & AWS SDKs

Para visualizar a política de exclusão dos serviços de IA em vigor para uma conta

Você pode usar uma das seguintes opções para visualizar a política de exclusão dos serviços de IA em vigor:

- AWS CLI: describe-effective-policy

O exemplo a seguir mostra a política de exclusão dos serviços de IA em vigor para uma conta.

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWS SDKs: DescribeEffectivePolicy

## Sintaxe e exemplos de política de exclusão dos serviços de IA

Este tópico descreve a sintaxe da política de exclusão de serviços de Inteligência Artificial (IA) e fornece exemplos.

Sintaxe para políticas de exclusão dos serviços de IA

Uma política de exclusão dos serviços de IA é um arquivo de texto sem formatação estruturado de acordo com as regras de JSON. A sintaxe para políticas de exclusão dos serviços de IA segue a sintaxe para os tipos de política de gerenciamento. Para ver uma discussão completa sobre essa sintaxe, consulte Entendendo a herança da política de gerenciamento. Este tópico se concentra na aplicação dessa sintaxe geral aos requisitos específicos do tipo de política de exclusão dos serviços de IA.

> **Important**
>
> O uso de maiúsculas e minúsculas nos valores discutidos nesta seção é importante. Insira os valores com letras maiúsculas e minúsculas, conforme mostrado neste tópico. As políticas não funcionam se você usar maiúsculas e minúsculas não previstas.

A política a seguir mostra a sintaxe básica de política de exclusão dos serviços de IA. Se este exemplo fosse anexado diretamente a uma conta, essa conta seria explicitamente excluída de um

serviço e incluída em outro. Outros serviços podem ser incluídos ou excluídos por políticas herdadas de níveis mais altos (UO ou políticas-raiz).

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Imagine o seguinte exemplo de política anexada à raiz da organização. Ele define como padrão que a organização opte pela exclusão de todos os serviços de IA. Isso inclui automaticamente quaisquer serviços de IA que não sejam explicitamente definidos como exceções de algum outro modo, incluindo quaisquer serviços de IA que a AWS possa vir a implantar no futuro. Você pode anexar políticas subordinadas a UOs ou diretamente a contas para substituir essa configuração para qualquer serviço de IA, exceto o Amazon Comprehend. A segunda entrada no exemplo a seguir usa `@@operators_allowed_for_child_policies` definido como `none` para evitar que seja substituído. A terceira entrada no exemplo faz uma exceção em toda a organização para o Amazon Rekognition. Ela opta por esse serviço para toda a organização, mas a política permite que políticas subordinadas prevaleçam quando apropriado.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
```

```
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

A sintaxe da política de exclusão dos serviços de IA inclui os seguintes elementos:

- O elemento `services`. Uma política de exclusão dos serviços de IA é identificada por esse nome fixo como o elemento mais externo que contém JSON.

  Uma política de exclusão dos serviços de IA pode ter uma ou mais instruções sob o elemento `services`. Cada instrução contém os seguintes elementos:

  - Uma chave de nome de serviço que identifica um serviço de AWS IA. Estes são nomes de chave válidos para esse campo:
    - **`default`** – representa todos os serviços de IA disponíveis no momento e inclui implícita e automaticamente quaisquer serviços de IA que possam ser vir a ser adicionados no futuro.
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`
    - `codeguruprofiler`
    - `codewhisperer`
    - `comprehend`
    - `connectamd`
    - `connectoptimization`
    - `contactlens`
    - `datazone`
    - `entityresolution`
    - `frauddetector`
    - `glue`
    - `guardduty`
    - `lex`

- `polly`
- `q`
- `quicksightq`
- `rekognition`
- `securitylake`
- `textract`
- `transcribe`
- `translate`

Cada instrução de política identificada por uma chave de nome de serviço pode conter os seguintes elementos:

- A chave de `opt_out_policy`. Essa chave deve estar presente. Esta é a única chave que você pode colocar sob uma chave de nome de serviço.

  A chave `opt_out_policy` pode conter apenas o operador `@@assign` com um dos seguintes valores:

  - `optOut` – você opta por não ter conteúdo utilizado para o serviço de IA especificado.
  - `optIn` – você opta por ter o conteúdo utilizado para o serviço de IA especificado.

  > **Observações**
  >
  > - Não é possível usar os operadores de herança `@@append` e `@@remove` em políticas de exclusão dos serviços de IA.
  > - Não é possível usar o operador `@@enforced_for` em políticas de exclusão dos serviços de IA.

- Em qualquer nível, você pode especificar o operador `@@operators_allowed_for_child_policies` para controlar o que as políticas subordinadas podem fazer para substituir as configurações impostas pelas políticas superiores. Você pode especificar um dos seguintes valores:

  - `@@assign` – as políticas subordinadas desta política podem usar o operador `@@assign` para substituir o valor herdado por um valor diferente.
  - `@@none` – as políticas subordinadas desta política não podem alterar o valor.

O comportamento de `@@operators_allowed_for_child_policies` depende de onde você o coloca. Você pode usar os seguintes locais:

- Sob a chave `services` – controla se uma política subordinada pode adicionar ou alterar a lista de serviços na política em vigor.
- Sob a chave para um serviço de IA específico ou a chave `default` - controla se uma política subordinada pode adicionar ou alterar a lista de chaves sob esta entrada específica.
- Sob a chave `opt_out_policies` para um serviço específico – controla se uma política subordinada pode alterar apenas a configuração para este serviço específico.

## Exemplos de política de exclusão dos serviços de IA

As políticas de exemplo a seguir são apenas para fins informativos.

### Exemplo 1: Excluir todos os serviços de IA para todas as contas da organização

O exemplo a seguir mostra uma política que você pode anexar à raiz de sua organização para excluir os serviços de IA para as contas de sua organização.

> **Tip**
>
> Se você copiar o exemplo a seguir usando o botão copiar no canto superior direito do exemplo, a cópia não incluirá os números de linha. Ele está pronto para colar.

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] – O `"@@operators_allowed_for_child_policies": ["@@none"]` que está sob `services` impede que qualquer política subordinada adicione quaisquer novas secções para serviços individuais, exceto a seção `default` que já está lá. `Default` é o espaço reservado que representa "todos os serviços de IA".
- [2] – O `"@@operators_allowed_for_child_policies": ["@@none"]` que está sob `default` impede que qualquer política subordinada adicione quaisquer novas secções, exceto a seção `opt_out_policy` que já está lá.
- [3] – O `"@@operators_allowed_for_child_policies": ["@@none"]` que está sob `opt_out_policy` impede que as políticas subordinadas alterem o valor da configuração de `optOut` ou adicionem quaisquer configurações adicionais.

Exemplo 2: Definir uma configuração padrão da organização para todos os serviços, mas permitir que políticas subordinadas substituam a configuração para serviços individuais

O exemplo de política a seguir define um padrão, que abrange toda a organização, para todos os serviços de IA. O valor de `default` impede que uma política subordinada altere o valor de `optOut` para o serviço `default`, o espaço reservado para todos os serviços de IA. Se esta política for aplicada como uma política superior anexando-a à raiz ou a uma UO, as políticas subordinadas ainda poderão alterar a definição de opção de exclusão para serviços individuais, como mostrado na segunda política.

- Como não há `"@@operators_allowed_for_child_policies": ["@@none"]` sob a chave `services`, as políticas subordinadas podem adicionar novas secções para serviços individuais.
- O `"@@operators_allowed_for_child_policies": ["@@none"]` que está sob `default` impede que qualquer política subordinada adicione quaisquer novas secções, exceto a seção `opt_out_policy` que já está lá.
- O `"@@operators_allowed_for_child_policies": ["@@none"]` que está sob `opt_out_policy` impede que as políticas subordinadas alterem o valor da configuração de `optOut` ou adicionem quaisquer configurações adicionais.

Política principal de exclusão dos serviços de IA da raiz da organização

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
```

```
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

A política do exemplo a seguir pressupõe que a política do exemplo anterior esteja anexada à raiz da organização ou a uma UO superior, e que você anexe esse exemplo a uma conta afetada pela política superior. Ela substitui a configuração padrão de opção por exclusão e opta explicitamente pela inclusão apenas para o serviço Amazon Lex.

Política subordinada de exclusão dos serviços de IA

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

A política efetiva resultante para o Conta da AWS é que a conta opte apenas pelo Amazon Lex e opte por não receber todos os outros serviços de AWS IA devido à configuração de `default` exclusão herdada da política principal.

Exemplo 3: Definir uma política de exclusão dos serviços de IA em toda a organização para um único serviço

O exemplo a seguir mostra uma política de exclusão dos serviços de IA que define uma configuração de `optOut` para um único serviço de IA. Se esta política for anexada à raiz da organização, impedirá que qualquer política subordinada substitua a configuração de `optOut` para esse serviço específico. Outros serviços não são tratados por esta política, mas podem ser afetados por políticas subordinadas em outras UOs ou contas.

```
{
    "services": {
        "rekognition": {
```

```
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

## Políticas de backup

O AWS Backup permite que você crie planos de backup que definem como fazer backup de seus recursos da AWS. As regras do plano incluem uma variedade de configurações, como a frequência de backup, a janela de tempo durante a qual o backup ocorre, a Região da AWS que contém os recursos a serem incluídos no backup e o cofre no qual armazenar o backup. Você pode, então, aplicar um plano de backup a grupos de recursos da AWS identificados usando tags. Você também deve identificar uma função do AWS Identity and Access Management (IAM) que concede ao permissão ao AWS Backup para executar a operação de backup em seu nome.

Políticas de backup no AWS Organizations combinam todas essas partes em documentos de texto JSON. Você pode anexar uma política de backup a qualquer um dos elementos na estrutura da sua organização, como a raiz, unidades organizacionais (UOs) e contas individuais. O Organizations aplica regras de herança para combinar as políticas na raiz da organização, quaisquer UOs superiores ou anexadas à conta. Isso resulta em uma política de backup efetiva para cada conta. Esta política efetiva instrui o AWS Backup sobre como fazer backup de seus recursos da AWS automaticamente.

As políticas de backup oferecem controle granular sobre o backup de seus recursos em qualquer nível que sua organização exija. Por exemplo, você pode especificar em uma política anexada à raiz da organização que ser feito backup de todas as tabelas do Amazon DynamoDB. Essa política pode incluir uma frequência de backup padrão. Você pode, então, anexar uma política de backup a UOs que substituem a frequência de backup de acordo com os requisitos de cada UO. Por exemplo, a UO `Developers` pode especificar uma frequência de backup de uma vez por semana, enquanto a UO `Production` especifica uma vez por dia.

Você pode criar políticas de backup parciais que incluem individualmente apenas parte das informações necessárias para fazer backup de seus recursos com êxito. Pode anexar diferentes essas políticas a diferentes partes da árvore da organização, como a raiz ou uma UO superior, com a intenção de que essas políticas parciais sejam herdadas por UOs e contas de nível inferior. Quando o Organizations combina todas as políticas de uma conta usando regras de herança, a política em

vigor resultante deve ter todos os elementos necessários. Caso contrário, o AWS Backup considera a política não válida e não faz backup dos recursos afetados.

> **Important**
>
> O AWS Backup só pode executar um backup com sucesso quando ele for chamado por uma política efetiva completa que tenha todos os elementos necessários.
> Embora uma estratégia de política parcial, conforme descrito no parágrafo anterior, possa funcionar, se uma política em vigor de uma conta estiver incompleta, isso resultará em erros ou na impossibilidade de fazer backup de alguns recursos. Como estratégia alternativa, considere exigir que todas as políticas de backup sejam completas e válidas por si só.
> Use valores padrão fornecidos por políticas anexadas em níveis mais alto na hierarquia e substitua-os quando necessário em políticas filho, incluindo operadores de controle de herança filho.

O plano de backup em vigor para cada Conta da AWS da organização aparece no console do AWS Backup como um plano imutável para essa conta. Você pode visualizá-lo, mas não alterá-lo.

Quando o AWS Backup inicia um backup com base em um plano de backup criado por políticas, você pode ver o status do trabalho de backup no console do AWS Backup. Um usuário em uma conta-membro pode ver o status e quaisquer erros para os trabalhos de backup nessa conta-membro. Se você também habilitar acesso a serviço confiável com o AWS Backup, um usuário na conta de gerenciamento da organização poderá ver o status e os erros de todos os trabalhos de backup da organização. Para obter mais informações, consulte Habilitação de o gerenciamento entre contas no Guia do desenvolvedor do AWS Backup.

## Conceitos básicos sobre políticas de backup

Siga estas etapas para começar a usar as políticas de backup.

1. Saiba mais sobre as permissões que você deve ter para executar qualquer tarefas de política de backup.
2. Saiba mais sobre algumas das melhores práticas que recomendamos ao usar políticas de backup.
3. Ative políticas de backup para sua organização.
4. Crie uma política de backup.
5. Anexe a política de backup à raiz, UO ou conta da sua organização.

6. Exiba a política de backup efetiva combinada que se aplica a uma conta.

Para todas essas etapas, você faz login como usuário do IAM, assume uma função do IAM ou faz login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

Outras informações

- Aprenda sobre a sintaxe da política de backup e veja as políticas de exemplo

## Pré-requisitos e permissões para gerenciar políticas de backup

Esta página descreve os pré-requisitos e as permissões necessárias para gerenciar políticas de backup no AWS Organizations.

Tópicos

- Pré-requisitos para gerenciar políticas de backup
- Permissões para gerenciar políticas de backup

### Pré-requisitos para gerenciar políticas de backup

Para gerenciar políticas de backup em uma organização, é necessário o seguinte:

- A organização deve ter todos os recursos habilitados.
- Você deve fazer login na conta de gerenciamento de sua organização.
- Seu usuário ou função do AWS Identity and Access Management (IAM) precisa das permissões listadas na seção a seguir.

### Permissões para gerenciar políticas de backup

O exemplo de política do IAM a seguir fornece permissões para gerenciar todos os aspectos das políticas de backup em uma organização.

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

```
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre as políticas e as permissões do IAM, consulte o Manual do usuário do IAM.

## Melhores práticas para usar políticas de backup

AWSA recomenda as melhores práticas a seguir para usar as políticas de backup.

### Decidir uma estratégia de política de backup

Você pode criar políticas de backup em partes incompletas que são herdadas e mescladas para criar uma política completa para cada conta-membro. Se você fizer isso, corre o risco de acabar com

uma política efetiva que não esteja completa se fizer uma alteração em um nível sem considerar cuidadosamente o impacto da alteração em todas as contas abaixo desse nível. Para que isso seja evitado, recomendamos que, em vez disso, você verifique se as políticas de backup implementadas em todos os níveis são completas em si mesmas. Trate as políticas superiores políticas padrão que podem ser substituídos pelas configurações especificadas nas políticas subordinadas. Dessa forma, mesmo que uma política subordinada não exista, a política herdada fica completa e usa os valores padrão. Você pode controlar quais configurações podem ser adicionadas, alteradas ou removidas por políticas subordinadas usando os operadores de herança de controle de subordinados.

Como validar alterações na verificação de políticas de backup usando **`GetEffectivePolicy`**

Depois de fazer uma alteração em uma política de backup, verifique as políticas efetivas para contas representativas abaixo do nível em que você fez a alteração. Você pode visualizar a política em vigor usando o AWS Management Console ou usando a operação de API GetEffectivePolicy ou uma de suas variantes da AWS CLI ou do AWS SDK. Certifique-se de que a alteração feita tenha o impacto pretendido na política efetiva.

Comece simples e faça pequenas alterações

Para simplificar a depuração, comece com políticas simples e faça alterações em um item de cada vez. Valide o comportamento e o impacto de cada alteração antes de fazer a próxima alteração. Essa abordagem reduz o número de variáveis que você tem que considerar quando um erro ou resultado inesperado acontece.

Armazene cópias de seus backups em outras Regiões da AWS e em contas de sua organização

Para melhorar sua posição na recuperação de desastres, você pode armazenar cópias de seus backups.

- Uma região diferente – Se armazenar cópias d o backup emRegiões da AWS, você ajuda a proteger o backup contra corrompimento ou exclusão acidental na região original. Use a seção `copy_actions` da política para especificar um cofre em uma ou mais regiões da mesma conta em que o plano de backup é executado. Para fazer isso, identifique a conta usando o a variável `$account` quando você especificar o ARN do cofre de backup no qual a cópia do backup será armazenada. A variável `$account` é automaticamente substituída em tempo de execução pelo ID da conta em que a política de backup está sendo executada.
- Uma conta diferente – Se armazenar cópias de backup adicionais em Contas da AWS, você adiciona uma barreira de segurança que ajuda a proteger contra um agente mal-intencionado que comprometa uma de suas contas. Use a seção `copy_actions` da política para especificar um

cofre em uma ou mais contas de sua organização, separadas da conta em que o plano de backup é executado. Para fazer isso, identifique a conta usando o número do ID quando especificar o ARN do cofre de backup no qual a cópia do backup será armazenada.

Limitar o número de planos por política

É mais complicado solucionar problemas em políticas que contêm vários planos devido ao maior número de saídas que devem ser validadas. Em vez disso, faça com que cada política contenha apenas um plano de backup para simplificar a depuração e a solução de problemas. Depois, você pode adicionar políticas extras com outros planos para atender a outros requisitos. Essa abordagem ajuda a manter quaisquer problemas com um plano isolados em uma política, além de impedir que esses problemas compliquem a solução de problemas com outras políticas e seus planos.

Use conjuntos de pilhas para criar as funções de IAM e os cofres de backup necessários

Use a integração dos conjuntos de pilhas do AWS CloudFormation com o Organizations para criar automaticamente os cofres de backup e as funções do AWS Identity and Access Management (IAM) necessários em cada uma das contas-membro de sua organização. Você pode criar um conjunto de pilha que inclua os recursos que deseja que estejam automaticamente disponíveis em todas as contas da Conta da AWS de sua organização. Essa abordagem permite que você execute seus planos de backup com a garantia de que as dependências já foram atendidas. Para obter mais informações, consulte Criação de um conjunto de pilhas com permissões autogerenciadas no Manual do usuário do AWS CloudFormation.

Verifique seus resultados analisando o primeiro backup criado em cada conta

Ao fazer uma alteração em uma política, verifique o próximo backup criado após essa alteração para garantir que a alteração teve o impacto desejado. Essa etapa vai além de analisar a política em vigor e garante que o AWS Backup interprete suas políticas e implemente os planos de backup da maneira desejada.

## Criação, atualização e exclusão de políticas de backup

Neste tópico:

- Depois de habilitar as políticas de backup para sua organização, você pode criar uma política.
- Quando os requisitos de backup forem alterados, você poderá atualizar uma política existente.
- Quando você não precisar mais de uma política e depois de desvinculá-la de todas as unidades organizacionais (UOs) e contas, você poderá excluí-la.

## Como criar uma política de backup

**Permissões mínimas**

Para criar uma política de backup, você precisa de permissão para executar a seguinte ação:

- `organizations:CreatePolicy`

### AWS Management Console

Você pode criar uma política de backup no AWS Management Console de uma das duas maneiras:

- Um editor visual que permite escolher opções e gera o texto da política JSON para você.
- Um editor de texto que permite que você mesmo crie diretamente o texto da política JSON.

O editor visual facilita o processo, mas limita sua flexibilidade. É uma ótima maneira de criar suas primeiras políticas e se sentir confortável ao usá-las. Depois de entender como elas funcionam e de começar a ser limitado pelo que o editor visual fornece, você poderá adicionar recursos avançados às suas políticas editando você mesmo o texto da política JSON. O editor visual usa apenas o operador de definição de valor @@assign e não fornece qualquer acesso aos operadores de controle subordinados. Você só pode adicioná-los se editar manualmente o texto de política JSON.

Para criar uma política de backup

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Backup policies (Políticas de backup), escolha Create policy (Criar política).
3. Na página Create policy (Criar política), insira um nome de política e uma descrição, opcional, para a política.
4. (Opcional) você pode adicionar uma ou mais tags escolhendo Add tag (Adicionar tag) e inserindo uma chave e um valor opcional. Se deixar o valor em branco, ele é definido como uma sequência vazia, não `null`. É possível anexar até 50 tags a uma política. Para obter mais informações sobre marcação, consulte Marcando atributos AWS Organizations.

5. Você pode criar a política usando o Editor Visual, conforme descrito neste procedimento. Você também pode inserir ou colar texto de política na guia JSON . Para obter informações sobre a sintaxe de política de backup, consulte Sintaxe e exemplos de políticas de backup.

   Se você optar por usar o Editor Visual, selecione as opções de backup apropriadas para seu cenário. Um plano de backup consiste em três partes. Para obter mais informações sobre esses elementos do plano de backup, consulte Criação de um plano de backup e Atribuição de recursos no Guia do desenvolvedor do AWS Backup.

   a. Detalhes gerais do plano de backup

      - O Nome do plano de backup pode consistir apenas em caracteres alfanuméricos, hífen e sublinhados.
      - Você deve selecionar pelo menos uma Região do plano de backup na lista. O plano pode fazer backup de recursos somente nas Regiões da AWS selecionadas.

   b. Uma ou mais regras de backup que especificam como e quando o AWS Backup deve operar. Cada regra de backup define os seguintes itens:

      - Uma programação que inclui a frequência do backup e a janela de tempo em que o backup pode ocorrer.
      - O nome do cofre de backup a ser usado. O nome do cofre de backup pode consistir apenas em caracteres alfanuméricos, hífen e sublinhados. O cofre de backup deve existir antes que o plano possa ser executado com êxito. Crie o cofre usando o console do AWS Backup ou comandos da AWS CLI.
      - (Opcional) Uma ou mais regras de Copiar para região também copiam o backup para cofres em outras Regiões da AWS.
      - Um ou mais pares de chave de tag e valor a serem anexados aos pontos de recuperação de backup criados sempre que esse plano de backup for executado.
      - Opções de ciclo de vida que especificam quando o backup faz a transição para o armazenamento frio e quando o backup expira.

      Escolha Add rule (Adicionar regra) para adicionar cada regra necessária ao plano.

      Para obter mais informações sobre backup, consulte Regras de backup no Guia do desenvolvedor do AWS Backup.

   c. Uma atribuição de recurso que especifica os recursos dos quais o AWS Backup deve fazer backup com este plano. A atribuição é feita especificando pares de tags que o AWS Backup usa para localizar e combinar recursos

- O nome da atribuição do recurso pode consistir apenas em caracteres alfanuméricos, hífen e sublinhados.
- Especifique a função do IAM a ser usada pelo AWS Backup para executar o backup pelo nome.

  No console, você não especifica o nome do recurso da Amazon (ARN) inteiro. Você deve incluir o nome da função e o prefixo que especifica o tipo de função. Os prefixos são tipicamente `role` ou `service-role`, e eles são separados do nome da função por uma barra ('/'). Por exemplo, você pode inserir `role/MyRoleName` ou `service-role/MyManagedRoleName`. Isso é convertido em um ARN completo para você quando armazenado no JSON subjacente.

  > **Important**
  >
  > A função do IAM especificada já deve existir na conta à qual a política é aplicada. Caso contrário, o plano de backup pode iniciar com êxito trabalhos de backup, mas esses trabalhos de backup falharão.

- Especifique uma ou mais chaves de tag de recurso e valores de tag para identificar os recursos dos quais você deseja que seja feito backup. Se houver mais de um valor de tag, separe-os com vírgulas.

Selecione Add assignment (Adicionar atribuição) para adicionar cada atribuição de recurso configurada ao plano de backup.

Para obter mais informações, consulte Atribuir recursos a um plano de backup no Guia do desenvolvedor do AWS Backup.

6. Quando terminar de criar sua política, escolha Create policy (Criar política). A política aparecerá na lista de políticas de backup disponíveis.

AWS CLI & AWS SDKs

Para criar uma política de backup

Você pode usar um dos seguintes procedimentos para criar uma política de backup:

- AWS CLI: create-policy

Crie um plano de backup como texto JSON semelhante ao seguinte e armazene-o em um arquivo de texto. Para obter regras completas para a sintaxe, consulte Sintaxe e exemplos de políticas de backup.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII" ] }
                        }
                    }
                }
        }
```

```
    }
}
```

Esse plano de backup especifica que o AWS Backup deve fazer backup de todos os recursos nas Contas da AWS afetadas que estão nas Regiões da AWS especificadas e que têm a tag `dataType` com valor de `PII`.

Em seguida, importe o plano de backup do arquivo de política JSON para criar uma nova política na organização. Observe o ID da política no final do ARN da política na saída.

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWS SDKs: CreatePolicy

O que fazer em seguida

Depois de criar uma política de backup, você pode colocar sua política em vigor. Para isso, você pode anexar a política à raiz da organização, unidades organizacionais (UOs), Contas da AWS dentro da organização ou uma combinação de tudo isso.

Como atualizar uma política de backup

Quando faz login na conta de gerenciamento da sua organização, você pode editar uma política que exija alterações na sua organização.

**Permissões mínimas**

Para atualizar uma política de backup, você deve ter permissão para executar as seguintes ações:

- `organizations:UpdatePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política a ser atualizada (ou "*")
- `organizations:DescribePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política a ser atualizada (ou "*")

AWS Management Console

Para atualizar uma política de backup

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Backup policies (Políticas de backup), escolha o nome da política que deseja atualizar.
3. Escolha Editar política.
4. Você pode inserir um novo nome da política, descrição da política. Você pode alterar o conteúdo da política usando o Editor visual ou editando diretamente o JSON.
5. Quando terminar de atualizar a política, escolha Salvar alterações.

AWS CLI & AWS SDKs

Para atualizar uma política de backup

Você pode usar uma das seguintes opções para atualizar uma política de backup:

- AWS CLI: update-policy

  O exemplo a seguir renomeia uma política de backup.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
```

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

O exemplo a seguir adiciona ou muda a descrição de uma política de backup.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

O exemplo a seguir altera o documento de política JSON anexado a uma política de backup. Neste exemplo, o conteúdo é retirado de um arquivo chamado `policy.json` com o seguinte texto:

```
{
    "plans": {
        "PII_Backup_Plan": {
```

```
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII" ] }
                        }
                    }
                }
            }
        }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- AWS SDKs: UpdatePolicy

### Edição de tags anexadas a uma política de backup

Quando faz login na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a uma política de backup. Para obter mais informações sobre marcação, consulte Marcando atributos AWS Organizations.

> **Permissões mínimas**
>
> Para editar as tags anexadas a uma política de backup de sua organização da AWS, você deve ter as seguintes permissões:
>
> - `organizations:DescribeOrganization` (somente console – para navegar até a política)
> - `organizations:DescribePolicy` (somente console – para navegar até a política)
> - `organizations:TagResource`
> - `organizations:UntagResource`

#### AWS Management Console

Para editar as tags anexadas a uma política de backup

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

2. Página Backup policies (Políticas de backup)
3. Escolha o nome da política com as tags que você deseja editar.

   A página de detalhes da política é exibida.
4. Na guia Tags (Tags), selecione Manage tags (Gerenciar tags).
5. Você pode executar qualquer uma das seguintes ações nesta página:

   - Edite o valor de qualquer tag inserindo um novo valor sobre o antigo. Não é possível modificar a chave. Para alterar uma chave, você deve excluir a tag com a chave antiga e adicionar uma tag com a nova chave.
   - Remova uma tag existente escolhendo Remove (Remover).
   - Adicione um novo par de chave e valor de tag. Escolha Add tag (Adicionar tag) e insira o novo nome da chave e o valor opcional nas caixas fornecidas. Se você deixar a caixa Value (Valor) vazia, o valor é uma sequência vazia, não é `null`.
6. Escolha Save changes (Salvar alterações) depois de ter feito todas as adições, remoções e edições que deseja fazer.

AWS CLI & AWS SDKs

Para editar as tags anexadas a uma política de backup

Você pode usar um dos seguintes comandos para editar uma política de backup:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Como excluir uma política de backup

Quando faz login na conta de gerenciamento da sua organização, você pode excluir uma política que não seja mais necessária em sua organização.

Antes de excluir uma política, você deve primeiro desvinculá-la de todas as entidades anexadas.

> **Permissões mínimas**
>
> Para excluir uma política, você deve ter permissão para executar a seguinte ação:

- `organizations:DeletePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política a ser excluída (ou "*")

AWS Management Console

Para excluir uma política de backup

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Backup policies (Políticas de backup), escolha o nome da política que deseja excluir.
3. Você primeiro deve desvincular a política de backup que deseja excluir de todas as raízes, UOs e contas. Escolha a guia Targets (Alvos), escolha o botão de opção ao lado de cada raiz, UO ou conta que é mostrada na lista Targets (Alvos) e escolha Detach (Desvincular). Na caixa de diálogo de confirmação, escolha Detach (Desvincular). Repita até remover todos os alvos.
4. Escolha Delete (Excluir), no alto da página.
5. Na caixa de diálogo de confirmação, insira o nome da política e escolha Delete (Excluir).

AWS CLI & AWS SDKs

Para excluir uma política de backup

Você pode usar uma das seguintes opções para excluir uma política:

- AWS CLI: delete-policy

  O exemplo a seguir exclui a política especificada. Ele só funciona se a política não estiver anexada a nenhuma raiz, UO ou conta.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: DeletePolicy

## Como anexar e desanexar políticas de backup

Você pode usar políticas de backup em uma organização inteira, bem como em unidades organizacionais (UOs) e contas individuais. Lembre-se dos seguintes pontos:

- Quando você anexa uma política de backup à raiz da organização, a política se aplica a todas as UOs e contas-membro dessa raiz.
- Quando você anexa uma política de backup a uma UO, essa política se aplica às contas que pertencem à UO ou a alguma UO subordinada. Essas contas também estão sujeitas a qualquer política anexada à raiz da organização.
- Quando você anexa uma política de backup a uma conta, essa política se aplica somente a essa conta. A conta também está sujeita a qualquer política anexada à raiz da organização e a qualquer UO a que a conta pertence.

A agregação de quaisquer políticas de backup que a conta herda da raiz e das UOs superiores, bem como quaisquer políticas diretamente anexadas à conta, é a política em vigor. Para obter informações sobre como as políticas são mescladas à política efetiva, consulte Entendendo a herança da política de gerenciamento.

### Como anexar uma política de backup

Quando faz login na conta de gerenciamento da sua organização, você pode anexar uma política de backup à raiz, UO ou diretamente a uma conta da organização.

**Permissões mínimas**

Para anexar políticas de backup, você deve ter permissão para executar a seguinte ação:

- `organizations:AttachPolicy`

#### AWS Management Console

Você pode anexar uma política de backup navegando para a política ou para a raiz, UO ou conta que você deseja anexar à política.

Para anexar a política de backup navegando para uma raiz, UO ou conta

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue e escolha o nome da raiz, UO ou conta à qual você deseja anexar a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
3. Na guia Policies (Políticas), na entrada para Backup policies (Políticas de backup), escolha Attach (Anexar).
4. Encontre a política que você deseja e escolha Attach policy (Anexar política).

   A lista de políticas de backup anexadas na guia Policies (Políticas) é atualizada para incluir a nova adição. A política entra em vigor imediatamente.

Para anexar uma política de backup navegando até a política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Backup policies (Políticas de backup), escolha o nome da política que deseja anexar.
3. Na guia Targets (Alvos), selecione Attach (Anexar).
4. Escolha o botão de opção ao lado da raiz, UO ou conta à qual você deseja anexar a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
5. Escolha Attach policy (Anexar política).

   A lista de políticas de backup anexadas na guia Targets (Alvos) é atualizada para incluir a nova adição. A política entra em vigor imediatamente.

AWS CLI & AWS SDKs

Para anexar uma política de backup à raiz, UO ou conta da organização

Você pode usar um dos seguintes comandos para anexar uma política de backup:

- AWS CLI: attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- AWS SDKs: AttachPolicy

A política entra em vigor imediatamente.

### Como desanexar uma política de backup

Quando faz login na conta de gerenciamento da organização, você pode desvincular a política de backup da raiz, UO ou conta da organização à qual ela está anexada. Depois de desanexar uma política de backup de uma entidade, essa política não será mais aplicada a nenhuma conta afetada anteriormente pela entidade agora desanexada. Para separar uma política, conclua as seguintes etapas.

> **Permissões mínimas**
>
> Para desanexar uma política de backup da raiz da organização, UO ou conta, você deve ter permissão para executar a seguinte ação:
>
> - `organizations:DetachPolicy`

#### AWS Management Console

Você pode desvincular uma política de backup navegando até a política ou até a raiz, UO ou conta da qual você deseja desvincular a política.

Para desvincular uma política de backup navegando até a raiz, UO ou conta à qual ela está anexada

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

2. Na página Contas da AWS, navegue até a raiz, UO ou conta da qual você deseja desvincular uma política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja. Escolha o nome da raiz, UO ou conta.
3. Na guia Policies (Políticas), escolha o botão de opção ao lado da política de backup que você deseja desvincular e selecione Detach (Desvincular).
4. Na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

   A lista de política de backup anexada é atualizada. A política entra em vigor imediatamente.

Para desvincular uma política de backup navegando até a política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Backup policies (Políticas de backup, escolha o nome da política que você deseja desvincular de uma raiz, UO ou conta.
3. Na guia Targets (Alvos), escolha o botão de opção ao lado da raiz, UO ou conta da qual você deseja desvincular a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
4. Escolha Detach (Desvincular).
5. Na caixa de diálogo de confirmação, escolha Detach (Desvincular).

   A lista de política de backup anexada é atualizada. A política entra em vigor imediatamente.

AWS CLI & AWS SDKs

Para desvincular uma política de backup da raiz, UO ou conta da organização

Você pode usar um dos seguintes comandos para desvincular uma política:

- AWS CLI: detach-policy

  O exemplo a seguir desvincula uma política de uma UO.

```
$ aws organizations detach-policy \
```

```
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS SDKs: DetachPolicy

A política entra em vigor imediatamente.

## Como visualizar políticas de backup efetivas

Você pode visualizar a política de backup em vigor de uma conta no Console de gerenciamento do AWS, na API da AWS ou Interface de linha de comando da AWS. A seção a seguir fornece uma breve visão geral da política de backup em vigor, incluindo um exemplo.

Qual é a política de backup efetiva?

A política de backup em vigor especifica as configurações finais do plano de backup que se aplicam a uma Conta da AWS. Ela é a agregação de todas as políticas de backup que a conta herda, mais de qualquer política de backup diretamente anexada à conta. Quando você anexa uma política de backup à raiz da organização, ela se aplica a todas as contas da organização. Quando você anexa uma política de backup a uma unidade organizacional (UO), ela se aplica a todas as contas e UOs que pertencem à UO. Quando você anexa uma política diretamente a uma conta, ela se aplica somente a essa uma Conta da AWS.

Por exemplo, a política de backup anexada à raiz da organização pode especificar que todas as contas na organização façam backup de todas as tabelas do Amazon DynamoDB com uma frequência de backup padrão de uma vez por semana. Uma política de backup separada anexada diretamente a uma conta-membro com informações críticas em uma tabela pode substituir a frequência por um valor de uma vez por dia. A combinação dessas políticas de backup compreende a política de backup efetiva. Essa política de backup em vigor é determinada para cada conta da organização individualmente. O resultado, neste exemplo, é que todas as contas na organização fazem backup de suas tabelas do DynamoDB uma vez por semana, com exceção de uma conta que faz backup de suas tabelas diariamente.

Para obter informações sobre como as políticas de backup são combinadas na política final em vigor, consulte Entendendo a herança da política de gerenciamento.

## Visualização da política de backup em vigor

Você pode visualizar a política de backup em vigor para uma conta usando o AWS Management Console, a API da AWS ou o AWS Command Line Interface.

> **Permissões mínimas**
>
> Para visualizar a política de backup efetiva de uma conta, você deve ter permissão para executar as seguintes ações:
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations

### AWS Management Console

Para visualizar a política de backup em vigor para uma conta

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, escolha o nome da conta para a qual você deseja visualizar a política de backup em vigor. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a conta que você deseja.
3. Na guia Policies (Políticas), na seção Backup policies (Políticas de backup), escolha View the effective backup policy for this Conta da AWS (Visualizar a política de backup em vigor para esta Conta da AWS).

   O console exibe a política em vigor aplicada à conta especificada.

   > **Note**
   >
   > Não é possível copiar e colar uma política em vigor e usá-la como JSON para outra política de backup sem alterações significativas. Os documentos de política de backup devem incluir operadores de herança que especificam como cada configuração é mesclada na política em vigor final.

AWS CLI & AWS SDKs

Para visualizar a política de backup em vigor para uma conta

Você pode usar uma dos seguintes comandos para visualizar a política de backup em vigor:

- AWS CLI: describe-effective-policy

  O exemplo a seguir exibe os detalhes de uma política de backup.

```
$ aws organizations describe-effective-policy \
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::
$account:role/MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes
\":\"10080\",\"target_backup_vault_name\
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},
\"copy_actions\":{\"arn:aws:backup:us-east-1:$accou
nt:backup-vault:secondary-vault\":{\"lifecycle\":
{\"move_to_cold_storage_after_days\":\"10\",\"delete_after_days\":\"100\"
}}}}}}}"
    }
}
```

- AWS SDKs: DescribeEffectivePolicy

## Usando eventos AWS CloudTrail para monitorar políticas de backup em sua organização

Você pode usar eventos AWS CloudTrail para monitorar quando as políticas de backup são criadas, atualizadas ou excluídas de qualquer conta em sua organização AWS ou quando há um plano de backup organizacional inválido. Para obter mais informações, consulte Registrar eventos de gerenciamento entre contas no AWS BackupGuia do desenvolvedor.

# Sintaxe e exemplos de políticas de backup

Esta página descreve a sintaxe da política de backup e fornece exemplos.

## Sintaxe para políticas de backup

Uma política de backup é um arquivo de texto sem formatação estruturado de acordo com as regras do JSON. A sintaxe para políticas de backup segue a sintaxe para todos os tipos de política de gerenciamento. Para obter uma discussão completa sobre essa sintaxe, consulte Sintaxe de política e herança para tipos de política de gerenciamento. Este tópico se concentra na aplicação dessa sintaxe geral aos requisitos específicos do tipo de política de backup.

Essa massa de uma política de backup é o plano de backup e suas regras. A sintaxe do plano de backup em uma política de AWS Organizations backup é estruturalmente idêntica à sintaxe usada por AWS Backup, mas os nomes das chaves são diferentes. Nas descrições dos nomes de chave de política abaixo, cada um inclui o nome de chave de AWS Backup plano equivalente. Para obter mais informações sobre AWS Backup planos, consulte CreateBackupPlano Guia doAWS Backup desenvolvedor.

> **Note**
>
> Ao usar JSON, nomes de chave duplicados serão rejeitados. Se você quiser incluir vários planos, regras ou seleções em uma única política, verifique se o nome de cada chave é exclusivo.

Para que seja completa e funcional, uma política de backup efetiva deve incluir mais do que apenas um plano de backup com sua programação e regras. A política também deve identificar os Regiões da AWS recursos a serem copiados e a função AWS Identity and Access Management (IAM) que AWS Backup pode ser usada para realizar o backup.

A seguinte política funcionalmente completa mostra a sintaxe básica da política de backup. Se esse exemplo fosse anexado diretamente a uma conta, AWS Backup faria backup de todos os recursos dessa conta nas `eu-north-1` regiões `us-east-1` e que têm a tag `dataType` com um valor de `PII` ou`RED`. Ele faz backup desses recursos diariamente às 5h00 em `My_Backup_Vault` e também armazena uma cópia no `My_Secondary_Vault`. Ambos os cofres estão na mesma conta que o recurso. Ele também armazena uma cópia do backup em `My_Tertiary_Vault` em uma conta diferente, explicitamente especificada. Os cofres já devem existir em cada um dos especificados

Regiões da AWS para cada um Conta da AWS que recebe a política efetiva. Se alguns dos recursos do backup forem instâncias do EC2, o suporte ao Microsoft Volume Shadow Copy Service (VSS) será habilitado para os backups nessas instâncias. O backup aplica a tag `Owner:Backup` a cada ponto de recuperação.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
```

```
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
}
```

A sintaxe da política de backup inclui os seguintes componentes:

- Variáveis de `$account` – Em determinadas sequências de texto nas políticas, você pode usar a variável `$account` para representar a Conta da AWSatual. Quando AWS Backup executa um plano na política efetiva, ela substitui automaticamente essa variável pela corrente Conta da AWS na qual a política efetiva e seus planos estão sendo executados.

  > **Important**
  >
  > Você pode usar a variável `$account` somente em elementos de política que possam incluir um nome do recurso da Amazon (ARN), como aqueles que especificam o cofre de backup para armazenamento do backup ou a função do IAM com permissões para executar o backup.

  Por exemplo, o seguinte exige que `My_Vault` exista um cofre chamado em cada um ao Conta da AWS qual a política se aplica.

  ```
  arn:aws:backup:us-west-2:$account:vault:My_Vault"
  ```

  Recomendamos que você use conjuntos de AWS CloudFormation pilhas e sua integração com Organizations para criar e configurar automaticamente cofres de backup e funções do IAM para cada conta membro na organização. Para obter mais informações, consulte Criação de um conjunto de pilhas com permissões autogerenciadas no Manual do usuário doAWS CloudFormation .

- Operadores de herança – As políticas de backup podem usar operadores de definição de valores e operadores de controle de subordinados.

- `plans`

  No nível superior, a chave da política é a chave `plans`. Uma política de backup deve sempre começar com esse nome de chave fixo na parte superior do arquivo de política. Sob esta chave, você pode ter um ou mais planos de backup.

- Cada plano na chave de nível superior `plans` tem um nome de chave que consiste no nome do plano de backup atribuído pelo usuário. No exemplo anterior, o nome do plano de backup é `PII_Backup_Plan`. Você pode ter vários planos em uma política, cada um com suas próprias `rules`, `regions`, `selections` e `tags`.

Esse nome de chave do plano de backup em uma política de backup mapeia o valor da `BackupPlanName` chave em um AWS Backup plano.

Cada plano pode conter os seguintes elementos:

- `rules` – Esta chave contém uma coleção de regras. Cada regra se traduz em uma tarefa agendada, com uma hora de início e uma janela para fazer backup dos recursos identificados pelos elementos `selections` e `regions` na política de backup em vigor.
- `regions`— Essa chave contém uma lista de matriz de Regiões da AWS cujos recursos podem ser copiados por essa política.
- `selections` – Esta chave contém uma ou mais coleções de recursos (dentro da `regions` especificada) dos quais as `rules` especificadas fazem backup.
- `advanced_backup_settings` – Esta chave contém configurações específicas para backups em execução em determinados recursos.
- `backup_plan_tags` – Esta especifica as tags que são anexadas ao plano de backup propriamente dito.

- `rules`

A chave de política `rules` mapeia para a chave `Rules` em um plano do AWS Backup . Você pode ter uma ou mais regras sob a chave `rules`. Cada regra se torna uma tarefa agendada para executar um backup dos recursos selecionados.

Cada regra contém uma chave cujo nome de chave é o nome da regra. No exemplo anterior, o nome da regra é “My_Hourly_Rule”. O valor da chave de regra é a seguinte coleção de elementos de regra:

- `schedule_expression`— Essa chave de política é mapeada para a `ScheduleExpression` chave em um AWS Backup plano.

  Especifica a hora de início do backup. Essa chave contém o operador do valor de `@@assign` herança e um valor de string com uma expressão CRON que AWS Backup especifica quando iniciar uma tarefa de backup. O formato geral da sequência CRON é: "cron( )". Cada um é um número ou curinga. Por exemplo, `cron(0 5 ? * 1,3,5 *)` inicia o backup às 5 da manhã, todas as segundas, quartas e sextas-feiras. `cron(0 0/1 ? * * *)` inicia o backup a cada hora, todos os dias da semana.
- `target_backup_vault_name`— Essa chave de política é mapeada para a `TargetBackupVaultName` chave em um AWS Backup plano.

Especifica o nome do cofre de backup no qual armazenar o backup. Você cria o valor usando AWS Backup. Esta chave contém o operador de valor de herança `@@assign` e um valor de string com um nome de cofre.

> **Important**
>
> O cofre já deve existir quando o plano de backup é iniciado pela primeira vez. Recomendamos que você use conjuntos de AWS CloudFormation pilhas e sua integração com Organizations para criar e configurar automaticamente cofres de backup e funções do IAM para cada conta membro na organização. Para obter mais informações, consulte Criar um conjunto de pilhas com permissões autogerenciadas no Guia do usuário doAWS CloudFormation .

- `start_backup_window_minutes`— Essa chave de política é mapeada para a `StartWindowMinutes` chave em um AWS Backup plano.

  (Opcional) Especifica o número de minutos a aguardar antes de cancelar um trabalho que não é iniciado com êxito. Esta chave contém o operador de valor de herança `@@assign` e um valor com um número inteiro de minutos.

- `complete_backup_window_minutes` – Esta chave de política mapeia para a chave `CompletionWindowMinutes` em um plano do AWS Backup .

  (Opcional) Especifica o número de minutos após um trabalho de backup ser iniciado com êxito antes de ser concluído ou ser cancelado pelo AWS Backup. Esta chave contém o operador de valor de herança `@@assign` e um valor com um número inteiro de minutos.

- `enable_continuous_backup`— Essa chave de política é mapeada para a `EnableContinuousBackup` chave em um AWS Backup plano.

  (Opcional) Especifica se AWS Backup cria backups contínuos. `True`causa AWS Backup a criação de backups contínuos capazes de point-in-time restauração (PITR). `False`(ou não especificadas) causas AWS Backup para criar backups instantâneos.

> **Note**
>
> Como os backups habilitados para PITR podem ser mantidos por um máximo de 35 dias, você deve escolher `False` ou não especifique um valor se definir qualquer uma das opções a seguir:

- Definir `delete_after_days` como um valor maior que 35.
- Definir `move_to_cold_storage_after_days` como qualquer valor.

Para obter mais informações sobre backups contínuos, consulte P oint-in-time recovery no Guia doAWS Backup desenvolvedor.

- `lifecycle`— Essa chave de política é mapeada para a `Lifecycle` chave em um AWS Backup plano.

  (Opcional) Especifica quando esse backup é AWS Backup transferido para armazenamento refrigerado e quando ele expira.

  - `move_to_cold_storage_after_days` — Essa chave de política é mapeada para a `MoveToColdStorageAfterDays` chave em um AWS Backup plano.

    Especifica o número de dias após o backup antes de o AWS Backup mover o ponto de recuperação para o armazenamento frio. Esta chave contém o operador de valor de herança `@@assign` e um valor com um número inteiro de dias.

  - `delete_after_days`— Essa chave de política é mapeada para a `DeleteAfterDays` chave em um AWS Backup plano.

    Especifica o número de dias após o backup antes de o AWS Backup excluir o ponto de recuperação. Esta chave contém o operador de valor de herança `@@assign` e um valor com um número inteiro de dias. Se você fizer a transição de um backup para o armazenamento frio, ele deve permanecer lá por um mínimo de 90 dias; portanto, esse valor deve ser de no mínimo 90 dias maior do que o valor `move_to_cold_storage_after_days`.

- `copy_actions`— Essa chave de política é mapeada para a `CopyActions` chave em um AWS Backup plano.

  (Opcional) Especifica quem AWS Backup deve copiar o backup em um ou mais locais adicionais. Cada local de cópia de backup é descrito da seguinte forma:

  - Uma chave cujo nome identifica exclusivamente esta ação de cópia. Neste momento, o nome da chave deve ser o nome do recurso da Amazon (ARN) do cofre de backup. Esta chave contém duas entradas.
    - `target_backup_vault_arn` – Esta chave de política mapeia para a chave `DestinationBackupVaultArn` em um plano do AWS Backup .

(Opcional) Especifica o cofre no qual AWS Backup armazena uma cópia adicional do backup. O valor desta chave contém a propriedade operador de valor de herança de `@@assign` e o ARN do cofre.

- Para referenciar um cofre no Conta da AWS qual a política de backup está sendo executada, use a `$account` variável no ARN no lugar do número de ID da conta. Quando AWS Backup executa o plano de backup, ele substitui automaticamente a variável pelo número de ID da conta Conta da AWS na qual a política está sendo executada. Isso permite que o backup seja executado corretamente quando a política de backup se aplica a mais de uma conta de uma organização.
- Para referenciar um cofre em uma outra Conta da AWS da mesma organização, use o número de ID de conta real no ARN.

> **Important**
>
> - Se esta chave estiver ausente, será usada uma versão em minúsculas do ARN no nome da chave superior. Como os ARNs diferenciam maiúsculas de minúsculas, essa sequência pode não corresponder ao ARN real do cofre e o plano falha. Por esse motivo, recomendamos que você sempre forneça essa chave e valor.
> - O cofre de backup para o qual você deseja copiar o backup já deve existir da primeira vez que você iniciar o plano de backup. Recomendamos que você use os conjuntos de pilhas do AWS CloudFormation e sua integração com o Organizations para criar e configurar automaticamente cofres de backup e funções do IAM para cada conta-membro da organização. Para obter mais informações, consulte Criação de um conjunto de pilhas com permissões autogerenciadas no Manual do usuário doAWS CloudFormation .

- `lifecycle`— Essa chave de política é mapeada para a `Lifecycle` chave abaixo da `CopyAction` chave em um AWS Backup plano.

  (Opcional) Especifica quando essa cópia de um backup é AWS Backup transferida para um armazenamento frio e quando ela expira.

  - `move_to_cold_storage_after_days` – Esta chave de política mapeia para a chave `MoveToColdStorageAfterDays` em um plano do AWS Backup .

Especifica o número de dias após a ocorrência do backup antes de AWS Backup mover o ponto de recuperação para o armazenamento refrigerado. Esta chave contém o operador de valor de herança `@@assign` e um valor com um número inteiro de dias.

- `delete_after_days` – Esta chave de política mapeia para a chave `DeleteAfterDays` em um plano do AWS Backup .

  Especifica o número de dias após a ocorrência do backup antes de AWS Backup excluir o ponto de recuperação. Esta chave contém o operador de valor de herança `@@assign` e um valor com um número inteiro de dias. Se você fizer a transição de um backup para o armazenamento frio, ele deve permanecer lá por um mínimo de 90 dias; portanto, esse valor deve ser de no mínimo 90 dias maior do que o valor `move_to_cold_storage_after_days`.

- `recovery_point_tags`— Essa chave de política é mapeada para a `RecoveryPointTags` chave em um AWS Backup plano.

  (Opcional) Especifica as tags que são AWS Backup anexadas a cada backup criado a partir desse plano. O valor dessa chave contém um ou mais dos seguintes elementos:

  - Um identificador para este par de nome e valor de chave. Esse nome para cada elemento sob `recovery_point_tags` é o nome da chave de tag em letras minúsculas, mesmo se a `tag_key` tenha um tratamento de caracteres diferente. Este identificador não diferencia maiúsculas e minúsculas. No exemplo anterior, esse par de chaves foi identificado pelo nome `0wner`. Cada par de chaves contém os seguintes elementos:

    - `tag_key` – Especifica o nome da chave de tag a ser anexada ao plano de backup. Esta chave contém o operador de valor de herança `@@assign` e um valor de string. O valor diferencia maiúsculas de minúsculas.

    - `tag_value`: especifica o valor anexado ao plano de backup e associado à `tag_key`. Essa chave contém qualquer um dos operadores de valor de herança, e um ou mais valores para substituir, acrescentar ou remover da política efetiva. Os valores diferenciam maiúsculas de minúsculas.

- `regions`

  A chave `regions` de política especifica o Regiões da AWS que deve AWS Backup ser examinado para encontrar os recursos que correspondem às condições na `selections` chave. Essa chave contém qualquer um dos operadores de valor de herança e um ou mais valores de string para Região da AWS códigos, por exemplo:. `["us-east-1", "eu-north-1"]`

- `selections`

  A chave de política `selections` especifica os recursos dos quais as regras de plano fazem backup nesta política. Essa chave corresponde aproximadamente ao BackupSelectionobjeto em AWS Backup. Os recursos são especificados por uma consulta para nomes e valores de chave de tag correspondentes. A chave `selections` contém uma chave abaixo dela: `tags`.

  - `tags` – Especifica as tags que identificam os recursos e a função do IAM que têm permissão para consultar os recursos e fazer backup deles. O valor dessa chave contém um ou mais dos seguintes elementos:

    - Um identificador para este elemento de tag. Esse identificador em `tags` é o nome da chave de tag em letras minúsculas, mesmo que a tag a consultar tenha um tratamento de caracteres diferente. Este identificador não diferencia maiúsculas e minúsculas. No exemplo anterior, um elemento foi identificado pelo nome `My_Backup_Assignment`. Cada identificador em `tags` contém os seguintes elementos:

      - `iam_role_arn` – Especifica a função do IAM que tem permissão para acessar os recursos identificados pela consulta de tag nas Regiões da AWS especificadas pela chave `regions`. Esse valor contém o operador do valor de `@@assign` herança e um valor de string que contém o ARN da função. AWS Backup usa essa função para consultar e descobrir os recursos e realizar o backup.

        Você pode usar a variável `$account` no ARN no lugar do número de ID da conta. Quando o plano de backup é executado AWS Backup, ele substitui automaticamente a variável pelo número real de ID da conta Conta da AWS na qual a política está sendo executada.

        > **Important**
        >
        > A função já deve existir quando você iniciar o plano de backup pela primeira vez. Recomendamos que você use conjuntos de AWS CloudFormation pilhas e sua integração com Organizations para criar e configurar automaticamente cofres de backup e funções do IAM para cada conta membro na organização. Para obter mais informações, consulte Criação de um conjunto de pilhas com permissões autogerenciadas no Manual do usuário doAWS CloudFormation .

      - `tag_key` – Especifica o nome da chave de tag a ser pesquisado. Esta chave contém o operador de valor de herança `@@assign` e um valor de string. O valor diferencia maiúsculas de minúsculas.

    - `tag_value`— Especifica o valor que deve ser associado a um nome de chave que `tag_key` corresponda. AWS Backup inclui o recurso no backup somente se o `tag_key` e `tag_value` corresponderem. Essa chave contém qualquer um dos operadores de valor de herança, e um ou mais valores para substituir, acrescentar ou remover da política efetiva. Os valores diferenciam maiúsculas de minúsculas.

- `advanced_backup_settings` – Especifica configurações para cenários de backup específicos. Esta chave contém uma ou mais configurações. Cada configuração é uma sequência de objeto JSON com os seguintes elementos:
    - Nome da chave do objeto – Uma sequência que especifica o tipo de recurso ao qual as configurações avançadas a seguir se aplicam.
    - Valor do objeto – Uma sequência de objeto JSON que contém uma ou mais configurações de backup específicas do tipo de recurso associado.

  No momento, a única configuração de backup avançada compatível habilita os backups do Microsoft Volume Shadow Copy Service (VSS) para Windows ou SQL Server em execução em uma instância do Amazon EC2. O nome da chave deve ser o tipo de recurso `"ec2"` e o valor especifica que o suporte de `"windows_vss"` esteja `enabled` ou `disabled` para backups realizados nessas instâncias do Amazon EC2. Para obter mais informações sobre esse recurso, consulte Criação de um backup do Windows habilitado para VSS no Guia do desenvolvedor doAWS Backup .

  ```
  "advanced_backup_settings": {
      "ec2": {
          "windows_vss": {
              "@@assign": "enabled"
          }
      }
  }
  ```

- `backup_plan_tags` – Especifica as tags anexadas ao plano de backup propriamente dito. Isso não afeta as tags especificadas em nenhuma regra ou seleções.

  (Opcional) Você pode anexar tags aos planos de backup. O valor desta chave é uma coleção de elementos.

  O nome de chave para cada elemento sob `backup_plan_tags` é o nome da chave de tag em letras minúsculas, mesmo se a tag a consultar tenha um tratamento de caracteres diferente. Este

identificador não diferencia maiúsculas e minúsculas. O valor para cada uma dessas entradas consiste nas seguintes chaves:

- `tag_key` – Especifica o nome da chave de tag a ser anexada ao plano de backup. Esta chave contém o operador de valor de herança `@@assign` e um valor de string. Esse valor diferencia maiúsculas de minúsculas.
- `tag_value`: especifica o valor anexado ao plano de backup e associado à `tag_key`. Esta chave contém o operador de valor de herança `@@assign` e um valor de string. Esse valor diferencia maiúsculas de minúsculas.

### Exemplos de políticas de backup

As políticas de backup no exemplo a seguir são apenas para fins informativos. Em alguns dos exemplos a seguir, a formatação de espaço em branco JSON pode ser compactada para economizar espaço.

#### Exemplo 1: Política atribuída a um nó pai

O exemplo a seguir mostra uma política de backup atribuída a um dos nós pai de uma conta.

Política superior – Esta política pode ser anexada à raiz da organização ou a qualquer UO que seja superior a todas as contas pretendidas.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
```

```
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        }                    }
```

```
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {
                        "@@assign": "enabled"
                    }
                }
            }
        }
    }
}
```

Se nenhuma outra política for herdada ou anexada às contas, a política efetiva renderizada em cada política aplicável será Conta da AWS semelhante ao exemplo a seguir. A expressão CRON faz com que o backup seja executado uma vez por hora. O ID da conta 123456789012 será o ID de conta real para cada conta.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
```

```
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
```

```
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

Exemplo 2: Uma política pai é mesclada com uma política filho

No exemplo a seguir, uma política principal herdada e uma política secundária herdadas ou diretamente associadas a uma Conta da AWS fusão para formar a política efetiva.

Política superior – Esta política pode ser anexada à raiz da organização ou a qualquer UO superior.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
```

```
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII", "RED" ] }
                    }
                }
            }
        }
    }
}
```

Política subordinada – Esta política pode ser anexada diretamente à conta ou a uma UO em qualquer nível abaixo daquele ao qual a política superior está anexada.

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
```

```
                                "to_delete_after_days": { "@@assign": "365" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "MonthlyDatatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                        "tag_key": { "@@assign": "BackupType" },
                        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                    }
                }
            }
        }
    }
}
```

Política em vigor resultante – A política em vigor aplicada às contas contém dois planos, cada um com o seu próprio conjunto de regras e conjunto de recursos aos quais as regras devem ser aplicadas.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
```

```
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                            "tag_key": "dataType",
                            "tag_value": [ "PII", "RED" ]
                        }
                    }
                }
            },
            "Monthly_Backup_Plan": {
                "regions": [ "us-east-1", "eu-central-1" ],
                "rules": {
                    "monthly": {
                        "schedule_expression": "cron(0 5 1 * ? *)",
                        "start_backup_window_minutes": "480",
                        "target_backup_vault_name": "Default",
                        "lifecycle": {
                            "to_delete_after_days": "365",
                            "move_to_cold_storage_after_days": "30"
                        },
                        "copy_actions": {
                            "arn:aws:backup:us-east-1:$account:vault:Default" : {
                                "target_backup_vault_arn": {
                                    "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                                },
                                "lifecycle": {
                                    "move_to_cold_storage_after_days": "30",
                                    "to_delete_after_days": "365"
                                }
                            }
                        }
                    }
                },
                "selections": {
```

```
                "tags": {
                    "monthlydatatype": {
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
    }
}
```

Exemplo 3: Uma política pai impede quaisquer alterações por uma política filho

No exemplo a seguir, uma política pai herdada usa os operadores de controle filho para impor todas as configurações e impede que elas sejam alteradas ou substituídas por uma política filho.

Política superior – Esta política pode ser anexada à raiz da organização ou a qualquer UO superior. A presença de `"@@operators_allowed_for_child_policies": ["@@none"]` em cada nó da política significa que uma política filho não pode fazer alterações de nenhum tipo no plano. Uma política filho também não pode adicionar planos extras à política efetiva. Essa política se torna a política efetiva para cada UO e conta sob a UO à qual ela está anexada.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "to_delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "to_delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                }
                            }
                        }
```

```
                    }
                }
            },
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "ec2": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "windows_vss": {
                        "@@assign": "enabled",
                        "@@operators_allowed_for_child_policies": ["@@none"]
                    }
                }
            }
        }
    }
}
```

Política em vigor resultante Se existirem políticas de backup subordinadas, elas serão ignoradas e a política superior se tornará a política em vigor.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
```

```
    }
}
```

Exemplo 4: Uma política pai impede alterações em um plano de backup por uma política filho

No exemplo a seguir, uma política pai herdada usa os operadores de controle filho para impor as configurações para um único plano e impede que elas sejam alteradas ou substituídas por uma política filho. A política filho ainda pode adicionar planos extras.

Política superior – Esta política pode ser anexada à raiz da organização ou a qualquer UO superior. Este exemplo é semelhante ao exemplo anterior com todos os operadores de herança filho bloqueados, exceto no nível superior dos `plans`. A configuração `@@append` nesse nível permite que as políticas filho adicionem outros planos à coleção na política efetiva. Quaisquer alterações ao plano herdado ainda são bloqueadas.

As seções do plano estão truncadas para maior clareza.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

Política subordinada – Esta política pode ser anexada diretamente à conta ou a uma UO em qualquer nível abaixo daquele ao qual a política superior está anexada. Esta política filho define um novo plano.

As seções do plano estão truncadas para maior clareza.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
```

```
    }
}
```

Política em vigor resultante – A política em vigor inclui ambos os planos.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Exemplo 5: Uma política filho substitui as configurações numa política pai

No exemplo a seguir, uma política subordinada usa operadores de definição de valor para substituir algumas das configurações herdadas de uma política superior.

Política superior – Esta política pode ser anexada à raiz da organização ou a qualquer UO superior. Qualquer uma das configurações pode ser substituída por uma política filho porque o comportamento padrão, na ausência de um operador de controle filho que o impede, é permitir a política filho para `@@assign`, `@@append`, ou `@@remove`. A política pai contém todos os elementos necessários para um plano de backup válido; portanto, ele faz backup de seus recursos com êxito se for herdado como está.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
```

```
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

Política subordinada – A política subordinada inclui apenas as configurações que precisam ser diferentes da política superior herdada. Deve haver uma política superior herdada que forneça as outras configurações necessárias quando mescladas em uma política em vigor. Caso contrário,

a política de backup em vigor contém um plano de backup inválido que não fará backup de seus recursos conforme o esperado.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

Política em vigor resultante – A política em vigor inclui configurações de ambas as políticas, com as configurações fornecidas pela política subordinada substituindo as configurações herdadas da superior. Neste exemplo, ocorrem as seguintes alterações:

- A lista de regiões é substituída por uma lista completamente diferente. Se você quiser adicionar uma região à lista herdada, consulte `@@append` em vez de `@@assign` na política subordinada.
- AWS Backup executa a cada duas horas em vez de a cada hora.
- AWS Backup permite 80 minutos para que o backup seja iniciado em vez de 60 minutos.
- AWS Backup usa o `Default` cofre em vez de. `FortKnox`
- O ciclo de vida é estendido tanto para a transferência para o armazenamento frio quanto para a eventual exclusão do backup.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

# Políticas de tag

Você pode usar políticas de tag para manter tags consistentes, incluindo o tratamento preferencial de maiúsculas e minúsculas de chaves e valores de tag.

## O que são tags?

Tags são rótulos de atributo personalizados que você ou a AWS atribui aos recursos da AWS. Cada tag tem duas partes:

- Uma chave de tag (por exemplo `CostCenter`, `Environment` ou `Project`). Chaves de tag fazem distinção entre maiúsculas e minúsculas.
- Um campo opcional conhecido como um valor de tag (por exemplo, `111122223333` ou `Production`). Omitir o valor da tag é o mesmo que usar uma string vazia. Como chaves de tag, os valores das tags diferenciam maiúsculas de minúsculas.

O restante desta página descreve as políticas de tag. Para obter mais informações sobre tags, consulte os tópicos a seguir:

- Para obter informações gerais sobre marcação, incluindo convenções de nomenclatura e uso, consulte o Guia do usuário de recursos de marcação AWS.
- Para obter uma lista de serviços que oferecem suporte à atribuição de tags, consulte a Referência da API de atribuição de tags a grupos de recursos.
- Para obter informações sobre o uso de tags para categorizar recursos, consulte o whitepaper sobre as melhores práticas para a marcação de AWS recursos.
- Para obter informações sobre a atribuição de tags a recursos de Organizations, consulte Marcando atributos AWS Organizations.
- Para obter informações sobre como marcar recursos em outros AWS serviços, consulte a documentação desse serviço.

## O que são políticas de tag?

Aspolíticas de tag são um tipo de política que pode ajuda você a padronizar tags entre recursos nas contas da organização. Em uma política de tags, você especifica regras de atribuição de tags aplicáveis aos recursos quando eles contêm tags.

Por exemplo, uma política de tag pode especificar que, quando a tag `CostCenter` é anexada a um recurso, ela deve usar o tratamento de maiúsculas e minúsculas e os valores de tag definidos pela política de tag. Uma política de tags também pode definir que operações de atribuição de tags não compatíveis em tipos de recursos especificados sejam aplicadas. Em outras palavras, solicitações de atribuição de tags não compatíveis em tipos de recursos especificados são impedidas de serem concluídas. Os recursos sem tag ou as tags que não são definidas na política de tags não são avaliados quanto à conformidade com a política de tags.

Usar políticas de tag envolve trabalhar com vários serviços da AWS:

- Use o AWS Organizations para gerenciar as políticas de tag. Quando faz login na conta de gerenciamento da organização, você pode usar o Organizations para habilitar o recurso de políticas de tag. Você deve 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. Em seguida, você pode criar políticas de tag e anexá-las às entidades da organização a fim de colocar essas regras de atribuição de tags em vigor.
- Use a AWS Resource Groups para gerenciar a conformidade com as política de tag. Quando faz login em uma conta de sua organização, você pode usar o Resource Groups para localizar tags não compatíveis nos recursos na conta. Você pode corrigir tags não compatíveis no serviço da AWS onde você criou o recurso.

  Se você fizer login na conta de gerenciamento de sua organização, poderá exibir informações de compatibilidade para todas as contas da organização.

As políticas de tag estão disponíveis apenas em uma organização com todos os recursos habilitados. Para obter mais informações sobre o que é necessário para usar políticas de tag, consulte Pré-requisitos e permissões para gerenciar políticas de tag.

> **Important**
>
> Para começar a usar políticas de tag, a AWS recomenda enfaticamente que você siga o fluxo de trabalho de exemplo descrito em Conceitos básicos das políticas de tag antes de aplicar políticas de tag mais avançadas. É melhor entender os efeitos de anexar uma política de tags simples a uma única conta antes de expandir as políticas de tag para uma UO ou organização inteira. É especialmente importante compreender os efeitos de uma política de tag antes de aplicar a conformidade com qualquer política de tag. As tabelas na página

Conceitos básicos das políticas de tag também fornecem links para instruções sobre tarefas relacionadas a políticas mais avançadas.

## Pré-requisitos e permissões para gerenciar políticas de tag

Esta página descreve os pré-requisitos e as permissões necessárias para gerenciar políticas de tag no AWS Organizations.

Tópicos



### Pré-requisitos para gerenciar políticas de tag

O uso de políticas de tag requer o seguinte:

- A organização deve ter todos os recursos habilitados.
- Você deve fazer login na conta de gerenciamento de sua organização.
- Você precisa das permissões listadas em Permissões para gerenciar políticas de tag.

Para avaliar a conformidade com as políticas de tag, use o AWS Resource Groups. Para obter informações sobre os requisitos para avaliar a conformidade, consulte Pré-requisitos e Permissões no Guia do usuário do AWS Resource Groups.

### Permissões para gerenciar políticas de tag

O exemplo de política do IAM a seguir fornece permissões para gerenciar políticas de tag.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
```

```
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre as políticas e as permissões do IAM, consulte o Guia do usuário do IAM.

## Práticas recomendadas para usar políticas de tag

AWSA recomenda as seguintes práticas para o uso de políticas de tag.

### Decida sobre uma estratégia de capitalização de tag

Determine como você deseja usar maiúsculas e minúsculas nas tags e implemente consistentemente essa estratégia em todos os tipos de recursos. Por exemplo, decida se deseja usar `Costcenter`, `costcenter` ou `CostCenter` e use a mesma convenção para todas as tags. Para obter resultados consistentes em relatórios de conformidade, evite usar tags semelhantes com tratamento

inconsistente de maiúsculas e minúsculas. Essa estratégia ajudará você a definir as políticas de tag da organização.

Use o fluxo de trabalho recomendado

Comece de baixo criando uma política de tags simples. Em seguida, anexe-a a uma conta-membro que você pode usar para fins de teste. Use os fluxos de trabalho descritos em Conceitos básicos das políticas de tag.

Determine regras de marcação

Isso dependerá das necessidades da organização. Por exemplo, você talvez queira especificar que, quando uma tag `CostCenter` for anexada a segredos do AWS Secrets Manager, ela deverá usar o tratamento de maiúsculas e minúsculas especificado. Crie políticas de tag que definam tags compatíveis e as anexe às entidades da organização nas quais você deseja que essas regras de atribuição de tags estejam em vigor.

Eduque os administradores de contas

Quando estiver pronto para expandir o uso das políticas de tag, instrua os administradores de contas da seguinte forma:

- Comunique sua estratégia de atribuição de tags.
- Enfatize que os administradores precisam usar tags em tipos de recursos específicos.

  Isso é importante, pois os recursos sem tags não são mostrados como incompatíveis nos resultados de conformidade.
- Fornecer orientações sobre como verificar a conformidade com as política de tag. Instrua os administradores a localizar e corrigir tags incompatíveis em recursos em suas contas usando o procedimento descrito em Avaliação da conformidade de uma conta no Guia do usuário do AWS Resource Groups. Informe-os com que frequência você quer que eles verifiquem a conformidade.

Esteja atento ao aplicar a conformidade.

A aplicação da conformidade pode impedir que os usuários nas contas da organização atribuam tags aos recursos necessários. Primeiramente, revise as informações em Noções básicas sobre a aplicação. Consulte também os fluxos de trabalho descritos em Conceitos básicos das políticas de tag.

Considere a criação de um SCP para definir proteções em torno de solicitações de criação de recursos

Os recursos que nunca tiveram tags anexadas a eles não aparecem como incompatíveis nos relatórios. Os administradores de conta ainda podem criar recursos sem tags. Em alguns casos, você pode usar uma política de controle de serviço (SCP) para definir proteções em torno de solicitações de criação de recursos. Para obter um exemplo de SCP, consulte Exigir uma tag em recursos criados especificados. Para saber se um serviço da AWS oferece suporte a controle de acesso usando tags, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM. Procure os serviços que têm Yes (Sim) na coluna Authorization based on tag (Autorização baseada em tags). Selecione o nome do serviço para visualizar a documentação de controle de acesso e a autorização desse serviço.

## Conceitos básicos das políticas de tag

O uso de políticas de tags envolve trabalhar com vários AWS serviços. Para começar, revise as páginas a seguir. Em seguida, siga os fluxos de trabalho nesta página para se familiarizar com as política de tag e seus efeitos.

- Pré-requisitos e permissões para gerenciar políticas de tag
- Práticas recomendadas para usar políticas de tag

Usar políticas de tag pela primeira vez

Siga estas etapas para começar a usar política de tag pela primeira vez.

| Tarefa | Conta para fazer login | AWS console de serviço a ser usado |
| --- | --- | --- |
| Etapa 1: habilitar políticas de tag para a organização. | A conta de gerenciamento da organização.[1] | AWS Organizations |
| Etapa 2: criar uma política de tag.<br><br>Crie sua primeira política de tags de forma simples. Insira uma chave de tag no | A conta de gerenciamento da organização.[1] | AWS Organizations |

| Tarefa | Conta para fazer login | AWS console de serviço a ser usado |
| --- | --- | --- |
| tratamento de maiúscula e minúscula que você deseja usar e deixe todas as outras opções com a configuração padrão. | | |
| Etapa 3: anexar uma política de tag a uma única conta-membro que você pode usar para teste.<br><br>Será necessário fazer login nesta conta na próxima etapa. | A conta de gerenciamento da organização.[1] | AWS Organizations |
| Etapa 4: criar alguns recursos com tags compatíveis e alguns com tags incompatíveis. | A conta-membro que você está usando para fins de teste. | Qualquer AWS serviço com o qual você se sinta confortável. Por exemplo, é possível usar o AWS Secrets Manager e seguir o procedimento em Criar um segredo básico para criar segredos compatíveis e não compatíveis. |
| Etapa 5: visualizar a política de tag efetiva e avaliar o status de conformidade da conta. | A conta-membro que você está usando para fins de teste. | Resource Groups e o AWS serviço em que o recurso foi criado.<br><br>Se você criou recursos com tags compatíveis e não compatíveis, você verá as tags não compatíveis nos resultados. |

| Tarefa | Conta para fazer login | AWS console de serviço a ser usado |
| --- | --- | --- |
| Etapa 6: repetir o processo de localizar e corrigir problemas de conformidade até que os recursos na conta de teste estejam em conformidade com sua política de tag. | A conta-membro que você está usando para fins de teste. | Resource Groups e o AWS serviço em que o recurso foi criado. |
| A qualquer momento, você pode avaliar a conformidade em toda a organização. | A conta de gerenciamento da organização.[1] | Grupos de recursos |

[1] Você deve 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.

Expandir o uso de políticas de tag

Você pode executar as seguintes tarefas em qualquer ordem para expandir o uso das políticas de tag.

| Tarefa avançada | Conta para fazer login | AWS console de serviço a ser usado |
| --- | --- | --- |
| Crie políticas de tag mais avançadas.<br><br>Siga o mesmo processo definido para usuários iniciantes, mas tente outras tarefas. Por exemplo, defina chaves ou valores adicionais ou especifique um tratamento de maiúsculas e minúsculas diferente para uma chave de tag. | A conta de gerenciamento da organização.[1] | AWS Organizations |

| Tarefa avançada | Conta para fazer login | AWS console de serviço a ser usado |
| --- | --- | --- |
| Você pode usar as informaçõ es em Entendendo a herança da política de gerenciamento e Sintaxe de política de tag para criar políticas de tag mais detalhadas. | | |
| Anexe políticas de tag a contas ou UO adicionais.<br><br>Verifique a política de tag efetiva de uma conta depois de anexar mais políticas a ela ou a qualquer UO em que a conta seja membro. | A conta de gerenciamento da organização.[1] | AWS Organizations |
| Crie uma SCP para exigir o uso de tags quando alguém criar novos recursos. Para ver um exemplo, consulte Exigir uma tag em recursos criados especificados. | A conta de gerenciamento da organização.[1] | AWS Organizations |
| Continue avaliando o status de compatibilidade da conta em relação à política de tag em vigor à medida que ela for alterada. Corrija tags fora de conformidade. | Uma conta-membro com uma política de tags efetiva. | Resource Groups e o AWS serviço em que o recurso foi criado. |
| Avalie a conformidade em toda a organização. | A conta de gerenciamento da organização.[1] | Grupos de recursos |

[1] Você deve 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.

## Aplicar política de tag pela primeira vez

Para aplicar políticas de tag pela primeira vez, siga um fluxo de trabalho semelhante ao primeiro uso de políticas de tag e use uma conta de teste.

> **Warning**
>
> Esteja atento ao aplicar a conformidade. Certifique-se de que você entende os efeitos do uso de políticas de tag e siga o fluxo de trabalho recomendado. Teste como a aplicação funciona em uma conta de teste antes de expandi-la para mais contas. Caso contrário, você pode impedir que os usuários nas contas da organização atribuam tags aos recursos necessários. Para ter mais informações, consulte Noções básicas sobre a aplicação.

| Tarefas de aplicação | Conta para fazer login | AWS console de serviço a ser usado |
| --- | --- | --- |
| Etapa 1: criar uma política de tag.<br><br>Mantenha a aplicação da sua primeira política de tag simples. Insira uma chave de tag no tratamento de maiúsculas e minúsculas que você deseja usar e escolha a opção Prevent noncompliant operations for this tag (Impedir operações incompatíveis para esta tag). Em seguida, especifique um tipo de recurso no qual aplicá-la. Continuando o exemplo anterior, você pode optar por aplicá-la em senhas do Secrets Manager. | A conta de gerenciamento da organização.[1] | AWS Organizations |

| Tarefas de aplicação | Conta para fazer login | AWS console de serviço a ser usado |
| --- | --- | --- |
| Etapa 2: anexar uma política de tag a uma única conta de teste. | A conta de gerenciamento da organização.[1] | AWS Organizations |
| Etapa 3: tente criar alguns recursos com tags compatíveis e alguns com tags incompatíveis. Você não deve ter permissão para criar uma tag em um recurso do tipo especificado na política de tag com uma tag fora de conformidade. | A conta-membro que você está usando para fins de teste. | Qualquer AWS serviço com o qual você se sinta confortável. Por exemplo, é possível usar o AWS Secrets Manager e seguir o procedimento em Criar um segredo básico para criar segredos compatíveis e não compatíveis. |
| Etapa 4: avaliar o status de conformidade da conta em relação à política de tag efetiva e corrigir tags incompatíveis. | A conta-membro que você está usando para fins de teste. | Resource Groups e o AWS serviço em que o recurso foi criado. |
| Etapa 5: repetir o processo de localizar e corrigir problemas de conformidade até que os recursos na conta de teste estejam em conformidade com sua política de tag. | A conta-membro que você está usando para fins de teste. | Resource Groups e o AWS serviço em que o recurso foi criado. |
| A qualquer momento, você pode avaliar a conformidade em toda a organização. | A conta de gerenciamento da organização.[1] | Grupos de recursos |

[1] Você deve 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.

Criar, atualizar e excluir políticas de tag

Neste tópico:

- Depois de habilitar as políticas de tag para sua organização, você pode criar uma política.
- Quando seu requisitos de marcação mudarem, você pode atualizar uma política existente.
- Quando você não precisar mais de uma política e depois de desvinculá-la de todas as unidades organizacionais (UOs) e contas, você poderá excluí-la.

> **Important**
>
> Os recursos sem tag não são exibidos como incompatíveis nos resultados.

Criar uma política de tag

> **Permissões mínimas**
>
> Para criar políticas de tag, você precisa de permissão para executar a seguinte ação:
>
> - `organizations:CreatePolicy`

Você pode criar uma política de tag no AWS Management Console de uma destas duas maneiras:

- Um editor visual que permite escolher opções e gera o texto da política JSON para você.
- Um editor de texto que permite que você mesmo crie diretamente o texto da política JSON.

O editor visual facilita o processo, mas limita sua flexibilidade. É uma ótima maneira de criar suas primeiras políticas e se sentir confortável ao usá-las. Depois de entender como elas funcionam e de começar a ser limitado pelo que o editor visual fornece, você poderá adicionar recursos avançados às suas políticas editando você mesmo o texto da política JSON. O editor visual usa apenas o operador de definição de valor @@assign e não fornece qualquer acesso aos operadores de controle subordinados. Você só pode adicioná-los se editar manualmente o texto de política JSON.

AWS Management Console

Como criar uma política de tag

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Tag policies (Políticas de tag) escolha Create policy (Criar política).
3. Na página Create policy (Criar política), insira um nome de política e uma descrição, opcional, para a política.
4. (Opcional) Você pode adicionar uma ou mais tags ao próprio objeto política. Essas tags não fazem parte da política. Para fazer isso, escolha Add tag (Adicionar tag) e, em seguida, insira uma chave e um valor opcional. Se deixar o valor em branco, ele é definido como uma sequência vazia, não `null`. É possível anexar até 50 tags a uma política. Para obter mais informações, consulte Marcando atributos AWS Organizations.
5. Você pode criar a política de tags usando o Visual editor (Editor Visual) conforme descrito neste procedimento. Você também pode digitar ou colar uma política de tag na guia JSON. Para obter informações sobre sintaxe de política de tag, consulte Sintaxe de política de tag.

   Em New tag Key 1 (Nova chave de tag 1), especifique o nome de uma chave de tag a ser adicionada.
6. Em Tag key capitalization compliance (Compatibilidade de maiúsculas e minúsculas em chave de tag), deixe esta opção desmarcada (o padrão) para especificar que a política de tag superior deve definir o tratamento de maiúsculas e minúsculas para a chave de tag.

   Habilite esta opção se quiser impor uma definição de maiúsculas e minúsculas para a chave de tag usando esta política. Se você selecionar essa opção, a diferenciação de maiúsculas e minúsculas especificada em Tag Key (Chave de tag) substituirá o tratamento de maiúsculas e minúsculas especificado em uma política superior.

   Se uma política superior não existir e você não habilitar essa opção, somente chaves de tag com todos os caracteres minúsculos serão consideradas compatíveis. Para obter mais informações sobre herança de políticas superiores, consulte Entendendo a herança da política de gerenciamento.

> **Tip**
>
> Considere usar como guia a política de tags de exemplo mostrada em Exemplo 1: definir maiúsculas e minúsculas de chave de tag em toda a organização, na criação de uma política de tag que defina chaves de tag e o tratamento de maiúsculas e minúsculas. Anexe-a à raiz da organização. Posteriormente, você pode criar e anexar políticas de tag adicionais a UOs ou contas, a fim de criar outras regras de atribuição de tags.

7. Para Tag value compliance (Compatibilidade de valor de tag), habilite esta opção se quiser adicionar valores permitidos para esta chave de tag a quaisquer valores herdados de uma política superior.

   Por padrão, essa opção está desmarcada, o que significa que somente os valores herdados de uma política superior são considerados compatíveis. Se uma política pai não existir e você não especificar valores de tag, qualquer valor (incluindo nenhum valor) será considerado compatível.

   Para atualizar a lista de valores de tag aceitáveis, selecione Specify allowed values for this tag key (Especificar valores permitidos para esta chave de tag) e depois Specify values (Especificar valores). Quando solicitado, insira os novos valores e escolha Save changes (Salvar alterações).

8. Em Prevent noncompliant operations for this tag (Impedir operações não compatíveis para esta tag), deixe esta opção desmarcada (o padrão), a menos que você tenha experiência com o uso de políticas de tag. Verifique se você revisou as recomendações em Noções básicas sobre a aplicação e teste cuidadosamente. Caso contrário, você pode impedir que os usuários nas contas da organização atribuam tags aos recursos necessários.

   Se você quiser impor compatibilidade com essa chave de tag, marque a caixa de seleção e selecione, Specify allowed values (Especificar valores permitidos). Quando solicitado, selecione os tipos de recursos a serem incluídos na política. Em seguida, escolha Save changes (Salvar alterações).

> **Important**
>
> Quando você seleciona essa opção, todas as operações que manipulam tags para recursos dos tipos especificados só serão bem-sucedidas se a operação resultar em tags compatíveis com a política.

9. (Opcional) Para adicionar outra chave de tag a esta política de tag, escolha Add tag key (Adicionar chave de tag). Depois, execute as etapas de 6 a 9 para definir a chave de tag.
10. Quando terminar de criar sua política de tags, escolha Save changes (Salvar alterações).

AWS CLI & AWS SDKs

Como criar uma política de tag

Você pode usar um dos seguintes procedimentos para criar uma política de tags:

- AWS CLI: create-policy

  É possível usar qualquer editor de texto para criar a política de tag. Use a sintaxe JSON e salve a política de tag como um arquivo com qualquer nome e extensão em um local de sua escolha. As políticas de tag podem ter no máximo 2.500 caracteres, incluindo espaços. Para obter informações sobre sintaxe de política de tag, consulte Sintaxe de política de tag.

  Como criar uma política de tag

  1. Crie uma política de tag em um arquivo de texto semelhante ao seguinte:

     Conteúdo de `testpolicy.json`:

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            }
        }
    }
}
```

Esta política de tag define a chave de tag `CostCenter`. A tag pode aceitar qualquer valor ou nenhum valor. Uma política como essa significa que um recurso que possui a tag CostCenter anexada com ou sem um valor é compatível.

2. Crie uma política que contenha o conteúdo da política do arquivo. O espaço em branco extra na saída foi truncado para facilitar a leitura.

```
$ aws organizations create-policy \
    --name "MyTestTagPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n\n"
    }
}
```

- AWS SDKs: CreatePolicy

O que fazer em seguida

Depois de criar uma política de tags, você pode colocar suas regras de atribuição de tags em vigor. Para isso, anexe a política à raiz da organização, unidades organizacionais (UOs), Contas da AWS dentro da organização ou uma combinação de entidades da organização.

## Atualizar uma política de tag

**Permissões mínimas**

Para atualizar uma política de tag, você deve ter permissão para executar as seguintes ações:

- `organizations:UpdatePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política especificada (ou "*")
- `organizations:DescribePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política especificada (ou "*")

### AWS Management Console

Para atualizar uma política de tag

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Tag policie (Políticas de tag), escolha a política de tag que deseja atualizar.
3. Escolha Editar política.
4. Você pode inserir um novo nome da política, descrição da política. Você pode alterar o conteúdo da política usando o Editor visual ou editando o JSON.
5. Quando terminar de atualizar a política de tag, escolha Save changes (Salvar alterações).

### AWS CLI & AWS SDKs

Para atualizar uma política

Você pode usar uma das seguintes opções para atualizar uma política:

- AWS CLI: update-policy

  O exemplo a seguir renomeia uma política de tag.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
```

```
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

O exemplo a seguir adiciona ou altera a descrição de uma política de tag.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

O exemplo a seguir altera o documento de política JSON anexado a uma política de exclusão dos serviços de IA. Neste exemplo, o conteúdo é retirado de um arquivo chamado `policy.json` com o seguinte texto:

```
{
  "tags": {
```

```
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWS SDKs: UpdatePolicy

Edição de tags anexadas a uma política de backup

Quando faz login na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a uma política de tag. Para fazer isso, conclua as seguintes etapas.

Permissões mínimas

Para editar as tags anexadas a uma política de tag de sua organização da AWS, você deve ter as seguintes permissões:

- `organizations:DescribeOrganization` (somente console – para navegar até a política)
- `organizations:DescribePolicy` (somente console – para navegar até a política)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar as tags anexadas a uma política de exclusão dos serviços de IA

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Tag policies (Políticas de tag), escolha o nome da política com as tags que você deseja editar.
3. Na página de detalhes da política, escolha a guia Tags, depois escolha Manage tags (Gerenciar tags).
4. Você pode executar qualquer uma das seguintes ações nesta página:
   - Edite o valor de qualquer tag inserindo um novo valor sobre o antigo. Não é possível modificar a chave. Para alterar uma chave, você deve excluir a tag com a chave antiga e adicionar uma tag com a nova chave.
   - Remova uma tag existente escolhendo Remove (Remover).
   - Adicione um novo par de chave e valor de tag. Escolha Add tag (Adicionar tag) e insira o novo nome da chave e o valor opcional nas caixas fornecidas. Se você deixar a caixa Value (Valor) vazia, o valor é uma sequência vazia, não é `null`.
5. Escolha Save changes (Salvar alterações) depois de ter feito todas as adições, remoções e edições que deseja fazer.

AWS CLI & AWS SDKs

Para editar as tags anexadas a uma política de tag

Você pode usar um dos seguintes comandos para editar as tags anexadas a uma política de tag:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Excluir uma política de tag

Quando faz login na conta de gerenciamento da sua organização, você pode excluir uma política que não seja mais necessária em sua organização.

Antes de excluir uma política, você deve primeiro desvinculá-la de todas as entidades anexadas.

> **Permissões mínimas**
>
> Para excluir uma política de tag, você deve ter permissão para executar a seguinte ação:
>
> - `organizations:DeletePolicy`

AWS Management Console

Como excluir uma política de tag

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. 
3. Na página Tag policies (Políticas de tag), escolha a política de tag que deseja excluir.
4. Você primeiro deve desvincular a política que deseja excluir de todas as raízes, UOs e contas. Escolha a guia Targets (Alvos), escolha o botão de opção ao lado de cada raiz, UO ou conta que é mostrada na lista Targets (Alvos) e escolha Detach (Desvincular). Na caixa de diálogo de confirmação, escolha Detach (Desvincular).
5. Escolha Delete (Excluir), no alto da página.
6. Na caixa de diálogo de confirmação, insira o nome da política e escolha Delete (Excluir).

AWS CLI & AWS SDKs

Como excluir uma política de tag

Você pode usar uma das seguintes opções para excluir uma política:

- AWS CLI: delete-policy

  O exemplo a seguir exclui a política especificada. Ele só funciona se a política não estiver anexada a nenhuma raiz, UO ou conta.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: DeletePolicy

Anexar e desvincular políticas de tag

Você pode usar políticas de tag em uma organização inteira, bem como em unidades organizacionais (UOs) e contas individuais.

- Quando você anexa uma política de tags à raiz da organização, a política de tags se aplica a todas as UO e contas membros dessa raiz.
- Quando você anexa uma política de tag a uma UO, essa política se aplica às contas que pertencem à UO. Essas contas também estão sujeitas a qualquer política de tag anexada à raiz da organização.
- Quando você anexa uma política de tags a uma conta, essa política se aplica à conta. Além disso, essa conta está sujeita a qualquer política de tag anexada à raiz da organização, além de qualquer política de tag anexada a uma UO à qual a conta pertence.

A agregação de todas as políticas de tag que a conta herda, além de qualquer política de tag diretamente anexada à conta, é a política de tag efetiva. Para obter mais informações, consulte Entendendo a herança da política de gerenciamento.

> **Important**
>
> Os recursos sem tag não são exibidos como incompatíveis nos resultados.

Permissões mínimas

Para anexar políticas de tag, você deve ter permissão para executar a seguinte ação:

- `organizations:AttachPolicy`

### AWS Management Console

Você pode anexar uma política de tag navegando até a política ou até a raiz, UO ou conta à qual você deseja anexar a política.

Para anexar a política de tag navegando para uma raiz, UO ou conta

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue e escolha o nome da raiz, UO ou conta à qual você deseja anexar a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
3. Na guia Policies (Políticas), na entrada para Tagpolicies (Políticas de backup), escolha Attach (Anexar).
4. Encontre a política que você deseja e escolha Attach policy (Anexar política).

   A lista de políticas de tag anexadas na guia Policies (Políticas) é atualizada para incluir a nova adição. A política entra em vigor imediatamente.

Para anexar uma política de tag navegando até a política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Tag policies (Políticas de tag), escolha o nome da política que deseja anexar.
3. Na guia Targets (Alvos), selecione Attach (Anexar).
4. Escolha o botão de opção ao lado da raiz, UO ou conta à qual você deseja anexar a política. Talvez seja necessário expandir as UOs (escolha

)

para encontrar a UO ou a conta que você deseja.

5. Escolha Attach policy (Anexar política).

   A lista de políticas de tag anexadas na guia Targets (Alvos) é atualizada para incluir a nova adição. A política entra em vigor imediatamente.

AWS CLI & AWS SDKs

Como anexar uma política de tag à raiz da organização, UO ou conta

Você pode usar um dos seguintes procedimentos para anexar uma política de tags:

- AWS CLI: attach-policy

  O procedimento a seguir mostra como anexar a política de tag que você acabou de criar a uma única conta de teste.

  - Anexe a política de tag à conta de teste executando um comando como o exibido a seguir:

    ```
    $ aws organizations attach-policy \
        --target-id <account-id> \
        --policy-id p-a1b2c3d4e5
    ```

    Este comando não produz saída se for bem-sucedido.

- AWS SDKs: AttachPolicy

A política entra em vigor imediatamente.

O que fazer em seguida

Depois de anexar uma política de tag, você pode descobrir até que ponto os recursos da conta são compatíveis com essa política de tag. Para fazer isso, use o console do Resource Groups. Para obter informações, consulte Avaliando a conformidade de uma conta no Guia do usuário do AWS Resource Groups.

## Desanexar uma política de tags

Quando faz login na conta de gerenciamento de sua organização, você pode desvincular a política de tag da raiz da organização, UO ou conta à qual ela está conectada. Depois de desanexar uma política de tags de uma entidade, essa política não será mais aplicada a nenhuma conta afetada pela entidade agora desanexada. Para separar uma política, conclua as seguintes etapas.

**Permissões mínimas**

Para desanexar uma política de tag da raiz da organização, UO ou conta, você deve ter permissão para executar a seguinte ação:

- `organizations:DetachPolicy`

### AWS Management Console

Você pode desvincular uma política de tag navegando até a política ou até a raiz, UO ou conta da qual você deseja desvincular a política.

Para desvincular uma política de tag navegando até a raiz, UO ou conta à qual ela está anexada

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue até a raiz, UO ou conta da qual você deseja desvincular uma política. Talvez seja necessário expandir as UOs (escolha ▶) para encontrar a UO ou a conta que você deseja. Escolha o nome da raiz, UO ou conta.
3. Na guia Policies (Políticas), escolha o botão de opção ao lado da política de tag que você deseja desvincular e selecione Detach (Desvincular).
4. Na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

   A lista de políticas de tag anexada é atualizada. A política entra em vigor imediatamente.

Para desvincular uma política de tag navegando até a política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Tag policies (Políticas de tag), escolha o nome da política que você deseja desvincular de uma raiz, UO ou conta.
3. Na guia Targets (Alvos), escolha o botão de opção ao lado da raiz, UO ou conta da qual você deseja desvincular a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
4. Escolha Detach (Desvincular).
5. Na caixa de diálogo de confirmação, escolha Detach (Desvincular).

   A lista de políticas de tag anexada é atualizada. A política entra em vigor imediatamente.

AWS CLI & AWS SDKs

Como desanexar uma política de tag da raiz da organização, UO ou conta

Você pode usar um dos seguintes procedimentos para desanexar uma política de tag:

- AWS CLI: detach-policy
- AWS SDKs: DetachPolicy

A política entra em vigor imediatamente.

## Visualizar políticas de tag efetivas

Antes de começar a verificar o status de conformidade dos recursos com tag em uma conta, é recomendável determinar primeiro a política de tags efetiva para uma conta.

Qual é a política de tag efetiva?

A política de tags efetiva especifica as regras de atribuição de tags que se aplicam a uma conta. É a agregação de todas as políticas de tag que a conta herda, além de qualquer política de tag diretamente anexada à conta. Quando você anexa uma política de tags à raiz da organização, ela se

aplica a todas as contas na organização. Quando você anexa uma política de tag a uma UO, ela se aplica a todas as contas e UOs que pertencem à UO.

Por exemplo, a política de tag anexada à raiz da organização pode definir uma tag `CostCenter` com quatro valores compatíveis. Uma política de tag separada anexada à conta pode restringir a chave `CostCenter` a apenas dois dos quatro valores compatíveis. A combinação dessas políticas de tag inclui a política de tag efetiva. O resultado é que apenas dois dos quatro valores de tag compatíveis, definidos na política de tag da raiz da organização, são compatíveis com a conta.

Para obter mais informações e exemplos mais avançados de como as políticas de tag efetivas são geradas, consulte Entendendo a herança da política de gerenciamento.

Como visualizar a política de tag efetiva

Você pode visualizar a política de tag efetiva de uma conta no AWS Management Console, na API da AWS ou na AWS Command Line Interface.

> **Permissões mínimas**
>
> Para visualizar a política de tag efetiva de uma conta, você deve ter permissão para executar as seguintes ações:
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization`

AWS Management Console

Para visualizar a política de tag em vigor para uma conta

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, escolha o nome da conta para a qual você deseja visualizar a política de tag em vigor. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a conta que você deseja.

3. Na guia Policies (Políticas), na seção Tag policies (Políticas de tag, escolha View the effective backup policy for this Conta da AWS (Visualizar a política de tag em vigor para esta Conta da AWS).

   O console exibe a política em vigor aplicada à conta especificada.

   > **Note**
   >
   > Não é possível copiar e colar uma política em vigor e usá-la como JSON para outra política de tag sem alterações significativas. Documentos de política de tag devem incluir os operadores de herança que especificam como cada configuração é mesclada na política em vigor final.

AWS CLI & AWS SDKs

Para visualizar a política de tag em vigor para uma conta

Você pode usar uma das seguintes opções para visualizar a política de tag efetiva:

- AWS CLI: describe-effective-policy

  Para determinar quais regras de atribuição de tags são herdadas ou anexadas a uma conta, execute o seguinte na conta e salve os resultados em um arquivo:

```
$ aws organizations describe-effective-policy \
    --policy-type TAG_POLICY
{
    "EffectivePolicy": {
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],
\"tag_key\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
}
```

  Se uma política de tag for anexada à conta, bem como à raiz da organização ou a qualquer UO, a combinação de ambas as políticas definirá a política de tag em vigor na conta. Nesses

casos, executar `describe-effective-policy` na conta retorna o conteúdo mesclado de todas as políticas de tag na hierarquia da conta.

- AWS SDKs: DescribeEffectivePolicy

## Como usar o Amazon EventBridge para monitorar tags incompatíveis

Você pode usar o Amazon EventBridge, anteriormente Amazon CloudWatch Events, para monitorar quando tags incompatíveis são introduzidas. No evento de exemplo a seguir, o valor `"false"` da `tag-policy-compliant` indica que uma nova tag não está em conformidade com a política de tag efetiva.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

Você pode se inscrever em eventos e especificar strings ou padrões a serem monitorados. Para obter mais informações sobre o EventBridge, consulte o Guia do usuário do Amazon EventBridge.

## Noções básicas sobre a aplicação

Uma política de tags pode definir que operações de atribuição de tags não compatíveis em tipos de recursos especificados sejam aplicadas. Em outras palavras, solicitações de atribuição de tags não compatíveis em tipos de recursos especificados são impedidas de serem concluídas.

> **Important**
>
> A imposição não tem efeito nos recursos criados sem tags.

Para aplicar a conformidade com políticas de tag, execute um dos procedimentos a seguir ao criar uma política de tags:

- Na guia Visual editor (Editor visual), selecione Impedir operações não compatíveis para esta tag.
- Na guia JSON, use o campo `enforced_for`. Para obter informações sobre a sintaxe da política de tag, consulte Sintaxe e exemplos de políticas de tag.

Siga as melhores práticas descritas a seguir para aplicar a conformidade com as políticas de tag:

- Tenha cuidado ao aplicar a compatibilidade – certifique-se de entender os efeitos do uso das políticas de tag e siga os fluxos de trabalho recomendados descritos em Conceitos básicos das políticas de tag. Teste como a aplicação funciona em uma conta de teste antes de expandi-la para mais contas. Caso contrário, você pode impedir que os usuários nas contas da organização atribuam tags aos recursos necessários.
- Saiba quais tipos de recursos você pode aplicar – você só pode impor a compatibilidade com as políticas de tag em tipos de recursos suportados. Os tipos de recursos que são compatíveis com a aplicação da conformidade são listados quando você usa o editor visual para criar uma política de tag.
- Entenda as interações com alguns serviços — Alguns AWS serviços têm agrupamentos de recursos semelhantes a contêineres que criam recursos automaticamente para você, e as tags podem se propagar de um recurso em um serviço para outro. Por exemplo, tags em grupos do Amazon EC2 Auto Scaling e clusters do Amazon EMR podem propagar-se automaticamente para as instâncias contidas do Amazon EC2. Você pode ter políticas de tag para o Amazon EC2 que são mais rigorosas do que as dos grupos do Auto Scaling ou os clusters do EMR. Se você habilitar a aplicação, a política de tag impede que os recursos sejam marcados e pode bloquear o dimensionamento dinâmico e o provisionamento.

As seções a seguir mostram como você pode encontrar recursos não compatíveis e corrigi-los para torná-los compatíveis.

Localizar recursos incompatíveis de uma conta

Para cada conta, você pode obter informações sobre recursos incompatíveis. Você deve executar esse comando de todas as regiões em que a conta tem recursos.

Para encontrar recursos não compatíveis para uma conta com uma política de tags, execute o comando a seguir para salvar os resultados em um arquivo:

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

Corrigir tags incompatíveis em recursos

Depois de encontrar tags incompatíveis, faça correções usando qualquer um dos seguintes métodos. Você deve estar conectado à conta que tem o recurso com tags incompatíveis:

- Use o console ou as operações de API de marcação do AWS serviço que criou os recursos não compatíveis.
- Use as UntagResourcesoperações AWS Resource Groups TagResourcese para adicionar tags que estejam em conformidade com a política efetiva ou para remover tags não compatíveis.

Localizar e corrigir problemas adicionais de incompatibilidade

Encontrar e corrigir problemas de conformidade é um processo iterativo. Repita as etapas nas duas seções anteriores até que os recursos com os quais você se preocupa estejam compatíveis com sua política de tag.

Gerar um relatório de conformidade em toda a organização

A qualquer momento, você pode gerar um relatório que lista todos os recursos marcados em Contas da AWS toda a sua organização. O relatório mostra se cada recurso está em conformidade com a política de tag efetiva. Observe que pode levar até 48 horas para que as alterações feitas em uma política de tag ou recursos sejam refletidas no relatório de conformidade de toda a organização. Por exemplo, suponha que você tenha uma política de tag que define uma nova tag padronizada para um tipo de recurso. Os recursos desse tipo que não têm essa tag são mostrados como compatíveis no relatório por até 48 horas.

Você pode gerar o relatório a partir da conta de gerenciamento da organização na região `us-east-1`, desde que ele tenha acesso a um bucket do Amazon S3. O bucket deve ter uma política

de bucket anexada, conforme mostrado em Política de bucket do Amazon S3 para relatório de armazenamento. Para gerar o relatório, execute o seguinte comando:

```
$ aws resourcegroupstaggingapi get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

Você pode gerar um relatório de cada vez.

Este relatório pode levar algum tempo para ser concluído. Você pode verificar o status executando o seguinte comando:

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

Depois que o comando acima retornar `SUCCEEDED`, você pode abrir o relatório no bucket do Amazon S3.

Serviços e tipos de recursos compatíveis com a aplicação

Os seguintes serviços e tipos de recursos são compatíveis com a aplicação de políticas de tag:

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
|---|---|---|
| Amazon API Gateway | • Chaves de API<br>• Nomes de domínio<br>• Novas operações de API REST<br>• Estágios | • `"apigateway:apikeys"`<br>• `"apigateway:domainnames"`<br>• `"apigateway:restapis"`<br>• `"apigateway:restapis/stages"` |
| AWS Amplify | • Componente | • `"amplifyuibuilder:app/environment/components"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| | • Tema | • `"amplifyuibuilder:app/environment/themes"` |
| AWS AppConfig | • Aplicativo<br>• Perfil de configuração<br>• Implantação<br>• Estratégia de implantação<br>• Ambiente | • `"appconfig:application"`<br>• `"appconfig:application/configurationprofile"`<br>• `"appconfig:application/environment/deployment"`<br>• `"appconfig:deploymentstrategy"`<br>• `"appconfig:application/environment"` |
| AWS App Mesh | • Todos<br>• Rota de gateway<br>• Mesh<br>• Rota<br>• Gateway virtual<br>• Nó virtual<br>• Roteador virtual<br>• Serviço virtual | • `"appmesh:*"`<br>• `"appmesh:mesh/virtualGateway/gatewayRoute"`<br>• `"appmesh:mesh"`<br>• `"appmesh:mesh/virtualRouter/route"`<br>• `"appmesh:mesh/virtualGateway"`<br>• `"appmesh:mesh/virtualNode"`<br>• `"appmesh:mesh/virtualRouter"`<br>• `"appmesh:mesh/virtualService"` |
| Amazon Athena | • Todos<br>• WorkGroup | • `"athena:*"`<br>• `"athena:workgroup"` |
| AWS Audit Manager | • Avaliação<br>• Framework de avaliação<br>• Controle | • `"auditmanager:assessment  "`<br>• `"auditmanager:assessmentFramework "`<br>• `"auditmanager:control  "` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| AWS Backup | • Plano de backup<br>• Cofre<br>• Gateway<br>• Hyper Visor<br>• VM | • `"backup:backup-plan"`<br>• `"backup:backup-vault"`<br>• `"backup-gateway:gateway"`<br>• `"backup-gateway:hypervisor"`<br>• `"backup-gateway:vm"` |
| AWS Batch | • Trabalho<br>• Definição da tarefa<br>• Job Queue | • `"batch:job"`<br>• `"batch:job-definition"`<br>• `"batch:job-queue"` |
| AWS BugBust | • Evento | • `"bugbust:event"` |
| AWS Certificate Manager | • Todos<br>• Certificados<br>• Private Certificate Authority | • `"acm:*"`<br>• `"acm:certificate"`<br>• `"acm-pca:certificate-authority"` |
| Amazon Chime | • Instância da aplicação<br>• Channel (Canal)<br>• Pipeline de mídia<br>• Reunião<br>• Aplicações de mídia de SIP<br>• Instância do aplicativo do usuário<br>• Conector de voz | • `"chime:app-instance"`<br>• `"chime:app-instance/channel"`<br>• `"chime:media-pipeline"`<br>• `"chime:meeting"`<br>• `"chime:sma"`<br>• `"chime:app-instance/user"`<br>• `"chime:vc"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| AWS Clean Rooms | • Colaboração<br>• Tabela configurada<br>• Associação<br>• Associação de tabela configurada | • `"cleanrooms:collaboration"`<br>• `"cleanrooms:configuredtable"`<br>• `"cleanrooms:membership"`<br>• `"cleanrooms:membership/configuredtableassociation"` |
| AWS Cloud9 | • Ambiente | • `"cloud9:environment"` |
| Amazon CloudFront | • Todos<br>• Distribuição<br>• Distribuição em streaming | • `"cloudfront:*"`<br>• `"cloudfront:distribution"`<br>• `"cloudfront:streaming-distribution"` |
| AWS CloudTrail | • Todos<br>• Trilha | • `"cloudtrail:*"`<br>• `"cloudtrail:trail"` |
| Amazon CloudWatch | • Todos<br>• Alarme<br>• Regra do Contributor Insights<br>• Fluxos de métricas | • `"cloudwatch:*"`<br>• `"cloudwatch:alarm"`<br>• `"cloudwatch:insight-rule"`<br>• `"cloudwatch:metric-stream"` |
| Monitor de CloudWatch Internet da Amazon | • Monitor | • `"internetmonitor:monitor"` |
| CloudWatch Registros da Amazon | • Destino<br>• Grupo de logs | • `"logs:destination"`<br>• `"logs:log-group"` |
| Gerenciador de acesso Amazon CloudWatch Observability | • Link<br>• Sink | • `"oam:link"`<br>• `"oam:sink"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| AWS CodeBuild | • Todos<br>• Projeto | • `"codebuild:*"`<br>• `"codebuild:project"` |
| Amazon CodeCatalyst | • Conexões | • `"codecatalyst:connections"` |
| AWS CodeCommit | • Todos<br>• Repositório | • `"codecommit:*"`<br>• `"codecommit:repository"` |
| AWS CodePipeline | • Todos<br>• Tipo de ação<br>• Pipeline<br>• Webhook | • `"codepipeline:*"`<br>• `"codepipeline:actiontype"`<br>• `"codepipeline:pipeline"`<br>• `"codepipeline:webhook"` |
| Identidade do Amazon Cognito | • Todos<br>• Grupo de identidades | • `"cognito-identity:*"`<br>• `"cognito-identity:identitypool"` |
| Grupos de usuários do Amazon Cognito | • Todos<br>• Grupo de usuários | • `"cognito-idp:*"`<br>• `"cognito-idp:userpool"` |
| Amazon Comprehend | • Todos<br>• Classificador de documentos<br>• Reconhecimento de entidade | • `"comprehend:*"`<br>• `"comprehend:document-classifier"`<br>• `"comprehend:entity-recognizer"` |
| AWS Config | • Todos<br>• Agregação de autorização<br>• Agregador de configuração<br>• Regra do Config | • `"config:*"`<br>• `"config:aggregation-authorization"`<br>• `"config:config-aggregator"`<br>• `"config:config-rule"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| CodeGuru Revisor da Amazon | • Associação | • `"codeguru-reviewer:association"` |
| CodeGuru Segurança da Amazon | • Verificar | • `"codeguru-security:scans"` |
| CodeConnections | • Conexão<br>• Host | • `"codestar-connections:connection"`<br>• `"codestar-connections:host"` |
| Amazon Connect | • Fluxo de contato<br>• Associação de integração<br>• Fila<br>• Conexão rápida<br>• Perfil de roteamento<br>• Usuário | • `"connect:instance/contact-flow"`<br>• `"connect:instance/integration-association"`<br>• `"connect:instance/queue"`<br>• `"connect:instance/transfer-destination"`<br>• `"connect:instance/routing-profile"`<br>• `"connect:instance/agent"` |
| Amazon Connect Wisdom | • Assistente<br>• Associação<br>• Conteúdo<br>• Base de conhecimento<br>• Sessão | • `"wisdom:assistant"`<br>• `"wisdom:association"`<br>• `"wisdom:content"`<br>• `"wisdom:knowledge-base"`<br>• `"wisdom:session"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| AWS Database Migration Service | • Todos<br>• Endpoint<br>• ES<br>• Rep<br>• Subgrp<br>• Tarefa | • `"dms:*"`<br>• `"dms:endpoint"`<br>• `"dms:es"`<br>• `"dms:rep"`<br>• `"dms:subgrp"`<br>• `"dms:task"` |
| Amazon Data Lifecycle Manager | • Política | • `"dlm:policy"` |
| AWS Diodo | • Mapeamento | • `"diode-messaging:mapping"` |
| AWS Direct Connect | • Todos<br>• Dxcon<br>• Dxlag<br>• Dxvif | • `"directconnect:*"`<br>• `"directconnect:dxcon"`<br>• `"directconnect:dxlag"`<br>• `"directconnect:dxvif"` |
| Amazon DynamoDB | • Todos<br>• Tabela | • `"dynamodb:*"`<br>• `"dynamodb:table"` |
| Amazon EC2 | • Reserva de capacidade<br>• Frota de reserva de capacidade<br>• Gateway da operadora | • `"ec2:capacity-reservation"`<br>• `"ec2:capacity-reservation-fleet"`<br>• `"ec2:carrier-gateway"` |
| | • Endpoint do cliente VPN<br>• Pool CoIP<br>• Gateway do cliente | • `"ec2:client-vpn-endpoint"`<br>• `"ec2:coip-pool"`<br>• `"ec2:customer-gateway"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| | • Host dedicado<br>• Opções do DHCP<br>• Gateway da Internet somente de saída | • `"ec2:dedicated-host"`<br>• `"ec2:dhcp-options"`<br>• `"ec2:egress-only-internet-gateway"` |
| | • Elastic IP<br>• Janela do evento<br>• Frota | • `"ec2:elastic-ip"`<br>• `"ec2:instance-event-window"`<br>• `"ec2:fleet"` |
| | • Imagem de FPGA<br>• Reserva de host<br>• Imagem | • `"ec2:fpga-image"`<br>• `"ec2:host-reservation"`<br>• `"ec2:image"` |
| | • Instância<br>• Gateway da Internet<br>• IP Address Manager | • `"ec2:instance"`<br>• `"ec2:internet-gateway"`<br>• `"ec2:ipam"` |
| | • Pool de gerenciamento de endereços IP<br>• Escopo do gerenciador de endereços IP<br>• Pool IPv4 | • `"ec2:ipam-pool"`<br>• `"ec2:ipam-scope"`<br>• `"ec2:ipv4pool-ec2"` |
| | • Par de chaves<br>• Modelo de execução<br>• Tabela de rotas do gateway local | • `"ec2:key-pair"`<br>• `"ec2:launch-template"`<br>• `"ec2:local-gateway-route-table"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| | • Associação de grupos de interface virtual da tabela de rotas do gateway local<br>• Associação VPC da tabela de rotas do gateway local<br>• nat gateway | • `"ec2:local-gateway-route-table-virtual-interface-group-association"`<br>• `"ec2:local-gateway-route-table-vpc-association"`<br>• `"ec2:natgateway"` |
| | • Conexão ACL<br>• Interface de rede<br>• Escopo de acesso do Network Insights | • `"ec2:network-acl"`<br>• `"ec2:network-interface"`<br>• `"ec2:network-insights-access-scope"` |
| | • Análise do escopo de acesso do Network Insights<br>• Análise do Network Insights<br>• Caminho do Network Insights | • `"ec2:network-insights-access-scope-analysis"`<br>• `"ec2:network-insights-analysis"`<br>• `"ec2:network-insights-path"` |
| | • Grupo de colocação<br>• Lista de prefixos<br>• Substituir tarefa de volume raiz | • `"ec2:placement-group"`<br>• `"ec2:prefix-list"`<br>• `"ec2:replace-root-volume-task"` |
| | • Instâncias reservadas<br>• Tabela de rotas<br>• Grupo de segurança | • `"ec2:reserved-instances"`<br>• `"ec2:route-table"`<br>• `"ec2:security-group"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| | • Snapshot<br>• Solicitações de instância Spot<br>• Sub-rede | • `"ec2:snapshot"`<br>• `"ec2:spot-instances-request"`<br>• `"ec2:subnet"` |
| | • Reserva CIDR de sub-rede<br>• Filtro de espelho de tráfego<br>• Sessão de espelho de tráfego | • `"ec2:subnet-cidr-reservation"`<br>• `"ec2:traffic-mirror-filter"`<br>• `"ec2:traffic-mirror-session"` |
| | • Destino de espelho de tráfego<br>• Gateway de trânsito<br>• Anexo do Transit Gateway | • `"ec2:traffic-mirror-target"`<br>• `"ec2:transit-gateway"`<br>• `"ec2:transit-gateway-attachment"` |
| | • Transit Gateway Connect Peer<br>• Domínio multicast do Transit Gateway<br>• Tabela de políticas do Transit Gateway | • `"ec2:transit-gateway-connect-peer"`<br>• `"ec2:transit-gateway-multicast-domain"`<br>• `"ec2:transit-gateway-policy-table"` |
| | • Tabela de rotas do gateway de trânsito<br>• Endpoint de acesso verificado<br>• Grupo de acesso verificado | • `"ec2:transit-gateway-route-table"`<br>• `"ec2:verified-access-endpoint"`<br>• `"ec2:verified-access-group"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| | • Instância de acesso verificada<br>• Provedor confiável de acesso verificado<br>• Volume | • `"ec2:verified-access-instance"`<br>• `"ec2:verified-access-trust-provider"`<br>• `"ec2:volume"` |
| | • Registro de fluxo de VPC<br>• VPC<br>• Endpoint da VPC | • `"ec2:vpc-flow-log"`<br>• `"ec2:vpc"`<br>• `"ec2:vpc-endpoint"` |
| | • Serviço de VPC endpoint<br>• Conexão de emparelhamento de VPC<br>• VPN connection (Conexão VPN)<br>• gateway VPN | • `"ec2:vpc-endpoint-service"`<br>• `"ec2:vpc-peering-connection"`<br>• `"ec2:vpn-connection"`<br>• `"ec2:vpn-gateway"` |
| Lixeira do Amazon EC2 | • Regra | • `"rbin:rule"` |
| AWS Elastic Beanstalk | • Aplicativo<br>• Versão da aplicação<br>• Modelo de configuração<br>• Plataforma | • `"elasticbeanstalk:application"`<br>• `"elasticbeanstalk:applicationversion"`<br>• `"elasticbeanstalk:configurationtemplate"`<br>• `"elasticbeanstalk:platform"` |
| Amazon Elastic Container Registry | • Repositório | • `"ecr:repository"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon Elastic Container Service | • Provedor de capacidade<br>• Cluster<br>• Serviço<br>• Definição de tarefa<br>• Conjunto de tarefas | • `"ecs:capacity-provider"`<br>• `"ecs:cluster"`<br>• `"ecs:service"`<br>• `"ecs:task-definition"`<br>• `"ecs:task-set"` |
| Amazon Elastic File System | • Todos<br>• Sistema de arquivos | • `"elasticfilesystem:*"`<br>• `"elasticfilesystem:file-system"` |
| Amazon Elastic Inference | • Accelerator | • `"elastic-inference:elastic-inference-accelerator"` |
| Amazon Elastic Kubernetes Service | • Cluster | • `"eks:cluster"` |
| Amazon ElasticSearch | • Domínio | • `"es:domain"` |
| Amazon EMR | • Cluster<br>• Editor | • `"elasticmapreduce:cluster"`<br>• `"elasticmapreduce:editor"` |
| Amazon EMR Serverless | • Aplicativo | • `"emr-serverless:applications"` |
| AWS Resolução de entidades | • Fluxo de trabalho de correspondência<br>• Mapeamento de esquemas | • `"entityresolution:matchingworkflow"`<br>• `"entityresolution:schemamapping"` |
| Amazon ElastiCache | • Cluster | • `"elasticache:cluster"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon EventBridge | • Todos<br>• Barramento de eventos<br>• Regra | • `"events:*"`<br>• `"events:event-bus"`<br>• `"events:rule"` |
| Amazon EventBridge Pipes | • Barra vertical | • `"pipes:pipe"` |
| Amazon EventBridge Scheduler | • Grupo de agendamento | • `"scheduler:schedule-group"` |
| Amazon Fraud Detector | • Detector<br>• Versão do detector<br>• Modelo<br>• Regra<br>• Variável | • `"frauddetector:detector"`<br>• `"frauddetector:detector-version"`<br>• `"frauddetector:model"`<br>• `"frauddetector:rule"`<br>• `"frauddetector:variable"` |
| Amazon Global Accelerator | • Accelerator | • `"globalaccelerator:accelerator"` |
| Elastic Load Balancing | • Todos<br>• Receptor<br>• Regra do ouvinte<br>• Load balancer<br>• Grupo de destino | • `"elasticloadbalancing:*"`<br>• `"elasticloadbalancing:listener"`<br>• `"elasticloadbalancing:listener-rule"`<br>• `"elasticloadbalancing:loadbalancer"`<br>• `"elasticloadbalancing:targetgroup"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon FSx | • Todos<br>• Backup<br>• Sistema de arquivos | • `"fsx:*"`<br>• `"fsx:backup"`<br>• `"fsx:file-system"` |
| Amazon GuardDuty | • Detector<br>• Filtro<br>• Conjunto de IPs<br>• Conjuntos de inteligência de ameaças | • `"guardduty:detector"`<br>• `"guardduty:detector/filter"`<br>• `"guardduty:detector/ipset"`<br>• `"guardduty:detector/threatintelset"` |
| AWS HealthLake | • Datastore | • `"healthlake:datastore  "` |
| AWS HealthOmics | • Armazenamento de anotações<br>• Versão do armazenamento de anotações<br>• Armazenamento de referência<br>• Referência<br>• Executar<br>• Grupo de execução<br>• Armazenamento de sequências<br>• Conjunto de leitura<br>• Armazenamento de variantes<br>• Fluxo de trabalho | • `"omics:annotationStore"`<br>• `"omics:annotationStore/version"`<br>• `"omics:referenceStore"`<br>• `"omics:referenceStore/reference"`<br>• `"omics:run"`<br>• `"omics:runGroup"`<br>• `"omics:sequenceStore"`<br>• `"omics:sequenceStore/readSet"`<br>• `"omics:variantStore"`<br>• `"omics:workflow"` |
| Amazon Inspector | • Filtro | • `"inspector2:filter "` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| AWS Identity and Access Management | • Perfil da instância<br>• MFA<br>• Provedor OIDC<br>• Política<br>• Provedor SAML<br>• Certificado de servidor | • `"iam:instance-profile"`<br>• `"iam:mfa"`<br>• `"iam:oidc-provider"`<br>• `"iam:policy"`<br>• `"iam:saml-provider"`<br>• `"iam:server-certificate"` |
| AWS IoT Analytics | • Todos<br>• Channel (Canal)<br>• Conjunto de dados<br>• Datastore<br>• Pipeline | • `"iotanalytics:*"`<br>• `"iotanalytics:channel"`<br>• `"iotanalytics:dataset"`<br>• `"iotanalytics:datastore"`<br>• `"iotanalytics:pipeline"` |
| AWS IoT Events | • Todos<br>• Modelo de detector<br>• Entrada | • `"iotevents:*"`<br>• `"iotevents:detectorModel"`<br>• `"iotevents:input"` |
| AWS IoT Fleet Hub | • Aplicativo | • `"iotfleethub:application"` |
| AWS IoT SiteWise | • Ativo<br>• Modelo de ativo | • `"iotsitewise:asset"`<br>• `"iotsitewise:asset-model  "` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| AWS IoT Greengrass | • Implantação em massa<br>• Definição do Connector<br>• Definição principal<br>• Definição de dispositivo<br>• Definição de função<br>• Definição de logger<br>• Definição de recurso<br>• Definição de assinatura | • `"greengrass:bulk"`<br>• `"greengrass:connectorsDefinition"`<br>• `"greengrass:coresDefinition"`<br>• `"greengrass:devicesDefinition"`<br>• `"greengrass:functionsDefinition"`<br>• `"greengrass:loggersDefinition"`<br>• `"greengrass:resourcesDefinition"`<br>• `"greengrass:subscriptionsDefinition"` |
| AWS Key Management Service | • Todos<br>• Chave | • `"kms:*"`<br>• `"kms:key"` |
| Amazon Kinesis | • Todos<br>• Aplicativo | • `"kinesisanalytics:*"`<br>• `"kinesisanalytics:application"` |
| Amazon Data Firehose | • Todos<br>• Fluxo de entrega | • `"firehose:*"`<br>• `"firehose:deliverystream"` |
| AWS Lambda | • Todos<br>• Função | • `"lambda:*"`<br>• `"lambda:function"` |
| Amazon Macie | • Identificador de dados personalizado | • `"macie2:custom-data-identifier"` |
| Amazon MediaStore | • Contêiner | • `"mediastore:container"` |
| Amazon MQ | • Agente<br>• Configuração | • `"mq:broker"`<br>• `"mq:configuration"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon Network Firewall | • Firewall<br>• Política de firewall<br>• Grupo de regras com estado<br>• Grupo de regras sem estado | • `"network-firewall:firewall"`<br>• `"network-firewall:firewall-policy"`<br>• `"network-firewall:stateful-rulegroup"`<br>• `"network-firewall:stateless-rulegroup"` |
| Amazon sem OpenSearch servidor | • Coleta | • `"aoss:collection"` |
| AWS Organizations | • Conta<br>• Unidade Organizacional<br>• Política<br>• Raiz | • `"organizations:account"`<br>• `"organizations:ou"`<br>• `"organizations:policy"`<br>• `"organizations:root"` |
| Amazon Pinpoint SMS Voice V2 | • Conjunto de configurações<br>• Lista de exclusão<br>• Número de telefone<br>• Grupo<br>• ID do remetente | • `"sms-voice:configuration-set"`<br>• `"sms-voice:opt-out-list"`<br>• `"sms-voice:phone-number"`<br>• `"sms-voice:pool"`<br>• `"sms-voice:sender-id"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon RDS | • Grupo de parâmetros do cluster<br>• Endpoint do cluster<br>• Assinatura de eventos<br>• Grupo de opções do banco de dados<br>• DB parameter group (grupo de parâmetros de banco de dados)<br>• Proxy de banco de dados<br>• Endpoint de proxy de banco de dados<br>• Instância de banco de dados reservada<br>• DB security group (grupo de segurança de banco de dados)<br>• DB subnet group (Grupo de subredes do banco de dados)<br>• Grupo de destino | • `"rds:cluster-pg"`<br>• `"rds:cluster-endpoint"`<br>• `"rds:es"`<br>• `"rds:og"`<br>• `"rds:pg"`<br>• `"rds:db-proxy"`<br>• `"rds:db-proxy-endpoint"`<br>• `"rds:ri"`<br>• `"rds:secgrp"`<br>• `"rds:subgrp"`<br>• `"rds:target-group"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon Redshift | • Todos<br>• Cluster<br>• Grupo de banco de dados<br>• Nome do banco de dados<br>• Usuário do banco de dados<br>• Assinatura de eventos<br>• Certificado do cliente HSM<br>• Configuração de HSM<br>• Grupo de parâmetros<br>• Snapshot<br>• Concessão de cópia de snapshot<br>• Programação de snapshots.<br>• Grupo de sub-rede | • `"redshift:*"`<br>• `"redshift:cluster"`<br>• `"redshift:dbgroup"`<br>• `"redshift:dbname"`<br>• `"redshift:dbuser"`<br>• `"redshift:eventsubscription"`<br>• `"redshift:hsmclientcertificate"`<br>• `"redshift:hsmconfiguration"`<br>• `"redshift:parametergroup"`<br>• `"redshift:snapshot"`<br>• `"redshift:snapshotcopygrant"`<br>• `"redshift:snapshotschedule"`<br>• `"redshift:subnetgroup"` |
| Amazon Redshift sem servidor | • Namespace<br>• WorkGroup | • `"redshift-serverless:namespace"`<br>• `"redshift-serverless:workgroup"` |
| AWS Resource Access Manager | • Todos<br>• Compartilhamento de recursos | • `"ram:*"`<br>• `"ram:resource-share"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| AWS Resource Groups | • Todos<br>• Grupo | • `"resource-groups:*"`<br>• `"resource-groups:group"` |
| Amazon Route 53 | • Zona hospedada | • `"route53:hostedzone"` |
| Amazon Route 53 Resolver | • Todos<br>• Endpoint do resolvedor<br>• Regra do resolvedor | • `"route53resolver:*"`<br>• `"route53resolver:resolver-endpoint"`<br>• `"route53resolver:resolver-rule"` |
| Amazon S3 | • Bucket<br>• Storage Lens<br>• Grupo de lentes de armazenamento | • `"s3:bucket"`<br>• `"s3:storage-lens"`<br>• `"s3:storage-lens-group"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon SageMaker | • Config de imagem de aplicativo<br>• Artifact<br>• Contexto<br>• Trabalho de treinamento<br>• Processamento de trabalho<br>• Grupo de pacotes modelo<br>• UI de tarefa humana<br>• Pacote de modelos<br>• Ação<br>• Pipeline<br>• Experimento<br>• Definição de fluxo<br>• Projeto | • `"sagemaker:app-image-config"`<br>• `"sagemaker:artifact"`<br>• `"sagemaker:context"`<br>• `"sagemaker:training-job"`<br>• `"sagemaker:processing-job "`<br>• `"sagemaker:model-package-group"`<br>• `"sagemaker:human-task-ui"`<br>• `"sagemaker:model-package"`<br>• `"sagemaker:action"`<br>• `"sagemaker:pipeline"`<br>• `"sagemaker:experiment"`<br>• `"sagemaker:flow-definition"`<br>• `"sagemaker:project"` |
| AWS Secrets Manager | • Todos<br>• Secreta | • `"secretsmanager:*"`<br>• `"secretsmanager:secret"` |
| AWS Lago de Segurança | • Data lake<br>• Assinante | • `"securitylake:data-lake"`<br>• `"securitylake:subscriber"` |
| AWS Service Catalog | • Aplicativo<br>• Grupo de atributos<br>• Portfólio<br>• Produto | • `"servicecatalog:applications"`<br>• `"servicecatalog:attribute-groups "`<br>• `"catalog:portfolio "`<br>• `"catalog:product "` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon Simple Notification Service (SNS) | • Tópico | • `"sns:topic"` |
| Amazon Simple Queue Service (SQS) | • Fila | • `"sqs:queue"` |
| Amazon States Language | • Todos<br>• Atividade<br>• State Machine (Máquina de estado) | • `"states:*"`<br>• `"states:activity "`<br>• `"states:stateMachine  "` |
| AWS Step Functions | • Atividade | • `"states:activity"` |
| AWS Storage Gateway | • Todos<br>• Gateway<br>• Compartilhar<br>• Fita<br>• Volume | • `"storagegateway:*"`<br>• `"storagegateway:gateway"`<br>• `"storagegateway:share"`<br>• `"storagegateway:tape"`<br>• `"storagegateway:gateway/volume"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| AWS Systems Manager | • Associação<br>• Execução de automação<br>• Documento<br>• Janela de manutenção<br>• Instância gerenciada<br>• Item de ops<br>• Lista de referência de patches<br>• Sessão<br>• Contatos | • `"ssm:association"`<br>• `"ssm:automation-execution"`<br>• `"ssm:document"`<br>• `"ssm:maintenancewindow"`<br>• `"ssm:managed-instance"`<br>• `"ssm:opsitem"`<br>• `"ssm:patchbaseline"`<br>• `"ssm:session"`<br>• `"ssm-contacts:contact"` |
| Amazon Textract | • Adaptadores<br>• Versões | • `"textract:adapters"`<br>• `"textract:adapters/versions"` |
| AWS Transfer Family | • Servidor<br>• Usuário<br>• Fluxo de trabalho | • `"transfer:server"`<br>• `"transfer:user"`<br>• `"transfer:workflow"` |
| Amazon Well-Architected | • Workload | • `"wellarchitected:workload"` |
| AWS Wickr | • Rede | • `"wickr:network"` |

| Nome do serviço | Tipo de recurso | Sintaxe do JSON |
| --- | --- | --- |
| Amazon WorkSpaces | • Todos<br>• Alias de conexão<br>• Diretório<br>• WorkSpace<br>• WorkSpaces pacote<br>• WorkSpaces imagem<br>• WorkSpaces Grupo IP | • `"workspaces:*"`<br>• `"workspaces:connectionalias"`<br>• `"workspaces:directory"`<br>• `"workspaces:workspace"`<br>• `"workspaces:workspacebundle"`<br>• `"workspaces:workspaceimage"`<br>• `"workspaces:workspaceipgroup"` |
| Amazon WorkLink | • Frota | • `"worklink:fleet"` |

## Sintaxe e exemplos de políticas de tag

Esta página fornece sintaxe e exemplos das políticas de tag.

Sintaxe de política de tag

Uma política de tag é um arquivo de texto sem formatação estruturado de acordo com as regras do JSON. A sintaxe para políticas de tag segue a sintaxe para os tipos de política de gerenciamento. Para ver uma discussão completa sobre essa sintaxe, consulte Entendendo a herança da política de gerenciamento. Este tópico se concentra na aplicação dessa sintaxe geral aos requisitos específicos do tipo de política de tag.

A seguinte política de tag mostra a sintaxe básica da política de tag:

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
```

```
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

A sintaxe da política de tag inclui os seguintes elementos:

- O nome da chave de campo `tags`. As políticas de tag sempre começam com esse nome de chave fixo. É a linha superior na política de exemplo acima.
- Uma chave de política que identifica exclusivamente a declaração da política. Ela deve corresponder ao valor da chave de tag, exceto para o tratamento de maiúsculas e minúsculas. Ao contrário da chave de tag (descrita em seguida), o valor da política não faz distinção entre maiúsculas e minúsculas.

  Neste exemplo, `costcenter` é a chave de política.
- Pelo menos uma chave de tag que especifica a chave de tag permitida com o uso de maiúsculas e minúsculas com o qual você deseja que os recursos sejam compatíveis. Se o tratamento de maiúsculas e minúsculas não está definido, o uso de minúsculas é o tratamento padrão para as chaves de tag. O valor da chave de tag deve corresponder ao valor da chave de política. Mas como o valor da chave de política não diferencia o uso de maiúsculas e minúsculas, os valores podem ser definidos de modo diferente.

  Neste exemplo, `CostCenter` é a chave de tag. Este é o tratamento de maiúsculas e minúsculas necessário para a conformidade com a política de tag. Os recursos com tratamento alternativo de maiúsculas e minúsculas para esta chave de tag não estão em conformidade com a política de tag.

  Você pode definir várias chaves de tag em uma política de tag.
- (Opcional) Uma lista de um ou mais valores de tag aceitáveis para a chave de tag. Se a política de tag não especificar um valor de tag para uma chave de tag, qualquer valor (incluindo nenhum valor) será considerado compatível.

  Neste exemplo, os valores aceitáveis para a chave de tag `CostCenter` são `100` e `200`.

- (Opcional) Uma opção `enforced_for` que indica se deve impedir qualquer operação de atribuição de tags incompatível em serviços e recursos especificados. No console, trata-se da opção Prevent noncompliant operations for this tag (Impedir operações incompatíveis para esta tag) no editor visual para criar políticas de tag. A configuração padrão para esta opção é nula.

  A política de tag de exemplo especifica que todos os recursos do AWS Secrets Manager devem ter essa tag.

  > **Warning**
  >
  > Você só deve alterar essa opção com a configuração padrão se tem experiência em usar políticas de tag. Caso contrário, você pode impedir que os usuários nas contas da organização criem os recursos necessários.

- Os operadores que especificam como a política de tag se mescla com outras políticas de tag dentro da árvore da organização para criar a política de tag efetiva de uma conta. Neste exemplo, `@@assign` é usado para atribuir strings a `tag_key`, `tag_value`, e `enforced_for`. Para obter mais informações sobre operadores, consulte Operadores de herança.
- – Você pode usar o caractere curinga `*` em valores de tag e campos de `enforced_for`.
  - Você só pode usar um caractere curinga por valor de tag. Por exemplo, `*@example.com` é permitido, mas `*@*.com` não é.
  - Para `enforced_for`, você pode usar o `<service>:*` com alguns serviços para habilitar a aplicação de todos os recursos desse serviço. Para obter uma lista de serviços e tipos de recursos que são compatíveis com `enforced_for`, consulte Serviços e tipos de recursos compatíveis com a aplicação.

    Não é possível usar um caractere curinga para especificar todos os serviços ou para especificar um recurso para todos os serviços.

Exemplos da política de tags

As políticas de tag de exemplo a seguir são apenas para fins informativos.

> **Note**
>
> Antes de tentar usar essas políticas de tag de exemplo em sua organização, observe o seguinte:

- Certifique-se de que seguiu o fluxo de trabalho recomendado para começar a usar as políticas de tag.
- Você deve revisar e personalizar cuidadosamente essas política de tag de acordo com seus requisitos exclusivos.
- Todos os caracteres em sua política de tags estão sujeitos a um tamanho máximo. Os exemplos deste guia mostram as políticas de tag formatadas com espaço em branco adicional para melhorar a legibilidade. No entanto, você pode excluir todos os espaços em branco para economizar espaço se o tamanho da política se aproximar ao tamanho máximo. Exemplos de espaço em branco incluem caracteres de espaço e quebras de linha que estão fora das aspas.
- Os recursos sem tag não são exibidos como incompatíveis nos resultados.

Exemplo 1: definir maiúsculas e minúsculas de chave de tag em toda a organização

O exemplo a seguir mostra uma política de tag que define apenas duas chaves de tag e o uso de maiúsculas e minúsculas que você deseja que as contas da organização usem como padrão.

Política A — Política de tag da raiz da organização

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Esta política de tag define duas chaves de tag: `CostCenter` e `Project` Anexar essa política de tag à raiz da organização tem os seguintes efeitos:

- Todas as contas em sua organização herdam essa política de tag.
- Todas as contas em sua organização devem usar o tratamento de maiúsculas e minúsculas definido para a conformidade. Os recursos com as tags `Project` `CostCenter` e estão em conformidade. Os recursos com tratamento alternativo de maiúsculas e minúsculas para a chave de tag (por exemplo, `costcenter`, `Costcenter` ou `COSTCENTER`) não estão em conformidade.
- As linhas `@@operators_allowed_for_child_policies": ["@@none"]` bloqueiam as chaves de tag. As políticas de tag anexadas mais abaixo na árvore da organização (políticas subordinadas) não podem usar operadores de definição de valor para alterar a chave de tag, incluindo o tratamento de maiúsculas e minúsculas.
- Assim como acontece com todas as políticas de tag, os recursos sem tag ou as tags que não estejam definidas na política de tag não são avaliados quanto à conformidade com a política de tag.

A AWS recomenda que você use este exemplo como guia na criação de uma política de tag semelhante para chaves de tag que deseja usar. Anexe-a à raiz da organização. Em seguida, crie uma política de tag semelhante ao exemplo a seguir, que define apenas os valores aceitáveis para as chaves de tag definidas.

Próxima etapa: definir valores

Suponha que anexou a política de tags anterior à raiz da organização. Em seguida, você pode criar uma política de tag como o exemplo a seguir e anexá-la a uma conta. Esta política define valores aceitáveis para as chaves de tag `CostCenter` e `Project`.

Política B – Política de tag de conta

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
```

```
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

Se você anexar a Política A à raiz da organização e a Política B a uma conta, as políticas são combinadas para criar a seguinte política de tag efetiva para a conta:

Política A + Política B = política de tag efetiva para a conta

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

Para obter mais informações sobre herança de política, incluindo exemplos de como os operadores de herança funcionam e exemplo de políticas de tag efetivas, consulte Entendendo a herança da política de gerenciamento.

Exemplo 2: impedir o uso de uma chave de tag

Para impedir o uso de uma chave de tag, você pode anexar uma política de tag como a seguinte a uma entidade da organização.

Esta política de exemplo especifica que nenhum valor é aceitável para a chave de tag `Color`. Ela também especifica que nenhum operador é permitido em políticas de tag filho. Portanto, qualquer

tag `Color` nos recursos das contas afetadas é considerada não compatíveis. Porém, a opção `enforced_for` na verdade impede somente que as contas afetadas marquem as tabelas do Amazon DynamoDB com a tag `Color`.

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

## Regiões compatíveis

Os recursos de política de tags estão disponíveis nas seguintes regiões:

| Nome da região | Parâmetro da região |
| --- | --- |
| Região Leste dos EUA (N. da Virgínia)[1] | **`us-east-1`** |
| Região Leste dos EUA (Ohio) | `us-east-2` |
| Região Leste dos EUA (Norte da Califórnia) | `us-west-1` |
| Região Oeste dos EUA (Oregon) | `us-west-2` |

| Nome da região | Parâmetro da região |
| --- | --- |
| Região África (Cidade do Cabo)[2] | `af-south-1` |
| Região Ásia-Pacífico (Hong Kong)[2] | `ap-east-1` |
| Região Ásia-Pacífico (Mumbai) | `ap-south-1` |
| Ásia-Pacífico (Hyderabad) [2] | `ap-south-2` |
| Asia Pacific (Tokyo) Region | `ap-northeast-1` |
| Região Ásia-Pacífico (Seul) | `ap-northeast-2` |
| Região Ásia-Pacífico (Osaka) | `ap-northeast-3` |
| Região Ásia-Pacífico (Singapura) | `ap-southeast-1` |
| Asia Pacific (Sydney) Region | `ap-southeast-2` |
| Região Ásia-Pacífico (Jacarta) [2] | `ap-southeast-3` |
| Ásia-Pacífico (Melbourne) [2] | `ap-southeast-4` |
| Oeste do Canadá (Calgary) [2] | `ca-west-1` |
| Região do Canadá (Central) | `ca-central-1` |
| Região Europa (Frankfurt) | `eu-central-1` |
| Região da Europa (Zurique) [2] | `eu-central-2` |
| Região Europa (Milão) | `eu-south-1` |
| Europa (Espanha) [2] | `eu-south-2` |
| Região Europa (Irlanda) | `eu-west-1` |
| Região Europa (Londres) | `eu-west-2` |
| Região Europa (Paris) | `eu-west-3` |

| Nome da região | Parâmetro da região |
| --- | --- |
| Região Europa (Estocolmo) | `eu-north-1` |
| Região do Oriente Médio (EAU) [2] | `me-central-1` |
| Região Oriente Médio (Bahrein)[2] | `me-south-1` |
| Região América do Sul (São Paulo) | `sa-east-1` |
| Israel (Tel Aviv) [2] | `il-central-1` |

[1]É preciso especificar a Região **`us-east-1`** ao chamar as seguintes operações do Organizations:

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- Qualquer outra operação na raiz da organização, como ListRoots.

Você também deve especificar a Região **`us-east-1`** ao chamar as seguintes operações de API de atribuição de tags de grupos de recursos que fazem parte do recurso de políticas de tag:

- DescribeReportCreation
- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> Para avaliar a compatibilidade com políticas de tag em toda a organização, também é necessário ter acesso a um bucket do Amazon S3 na região Leste dos EUA (Norte da Virgínia) para armazenamento de relatórios. Para obter mais informações, consulte a política de bucket do Amazon S3 para armazenamento de relatórios no Guia do usuário de  AWS recursos de marcação.

Essas regiões devem ser habilitadas manualmente. Para saber mais sobre como ativar e desativar Regiões da AWS, consulte Especificar qual Regiões da AWS conta pode ser usada no Guia de referência de gerenciamento deAWS contas. O console do Resource Groups não está disponível nessas regiões.

## Políticas de controle de serviço (SCPs)

As políticas de controle de serviço (SCPs) são um tipo de política organizacional que você pode usar para gerenciar permissões na sua organização. Os SCPs oferecem controle central sobre o máximo de permissões disponíveis para os usuários e funções do IAM na sua organização. As SCPs ajudam você a garantir que as suas contas permaneçam dentro das diretrizes de controle de acesso da sua organização. As SCPs estão disponíveis apenas em uma organização com todos os recursos habilitados. As SCPs não estarão disponíveis se sua organização tiver habilitado somente os recursos de faturamento consolidado. Para obter instruções sobre como habilitar SCPs, consulte Habilitar e desabilitar tipos de política.

Os SCPs não concedem permissões aos usuários do IAM e às funções do IAM na sua organização. Nenhuma permissão é concedida por uma SCP. Um SCP define uma barreira de permissão, ou define limites, nas ações que os usuários do IAM e as funções do IAM em sua organização podem realizar. Para conceder permissões, o administrador deve anexar políticas para controlar o acesso, como políticas baseadas em identidade que são anexadas a usuários e funções do IAM, e políticas baseadas em recursos que estão anexadas aos recursos em suas contas. As permissões efetivas são a interseção lógica entre o que é permitido pelo SCP e o que é permitido pelas políticas baseadas em identidade e recursos.

> **Important**
>
> SCPs não afetam usuários ou funções na conta de gerenciamento. Elas afetam apenas as contas-membro de sua organização.

Tópicos nesta página

- Uso de dados de acesso para melhorar as SCPs
- Tarefas e entidades não restringidas por SCPs
- Criar, atualizar e excluir de políticas de controle de serviço
- Anexar e desvincular políticas de controle de serviço
- Avaliação do SCP
- Sintaxe de SCP
- Exemplos de política de controle de serviço

## Teste de efeitos das SCPs

AWS recomenda fortemente que você não anexe SCPs à raiz da sua organização sem testar minuciosamente o impacto que a política tem nas contas. Em vez disso, crie uma UO para a qual você possa mover suas contas, uma por vez, ou pelo menos em pequenas quantidades, para garantir que não seja possível bloquear acidentalmente usuários nos serviços principais. Uma forma de determinar se um serviço é usado por uma conta é examinar os últimos dados acessados pelo serviço no IAM. Outra forma é usar AWS CloudTrail para registrar o uso do serviço no nível da API.

> **Note**
>
> Você não deve remover a AWSAccess política completa, a menos que a modifique ou substitua por uma política separada com ações permitidas, caso contrário, todas as AWS ações das contas dos membros falharão.

## Tamanho máximo das SCPs

Todos os caracteres em sua conta de SCP contam em relação ao seu tamanho máximo. Os exemplos deste guia mostram as SCPs formatadas com espaço em branco adicional para melhorar a legibilidade. No entanto, para economizar espaço quando o tamanho da política se aproximar do tamanho máximo, é possível excluir todos os espaços em branco, como caracteres de espaço e quebras de linhas, que estiverem fora das aspas.

> **Tip**
>
> Use o editor visual para criar sua SCP. Ele remove automaticamente os espaços em branco.

## Vinculando SCPs a diferentes níveis da organização

Para uma explicação detalhada de como os SCPs funcionam, consulte Avaliação do SCP

## Efeitos de SCP sobre permissões

Os SCPs são semelhantes às políticas de permissão AWS Identity and Access Management (IAM) e usam quase a mesma sintaxe. No entanto, uma SCP nunca concede permissões. Em vez disso, os SCPs são políticas JSON que especificam as permissões máximas para os usuários do IAM e as funções do IAM na sua organização. Para obter mais informações, consulte Lógica da avaliação de políticas no Guia do usuário do IAM.

- As SCPs afetam usuários e funções do IAM que são gerenciadas por contas que fazem parte da organização. As SCPs não afetam diretamente as políticas baseadas em recursos. Elas também não afetam usuários ou funções de contas de fora da organização. Por exemplo, considere um bucket do Amazon S3; que é de propriedade da conta A em uma organização. A política de bucket (uma política baseada em recursos) concede acesso a usuários da conta B fora da organização. A conta A tem uma SCP anexada. Essa SCP não se aplica aos usuários externos na conta B. A SCP se aplica somente aos usuários gerenciados pela conta A na organização.
- Uma SCP restringe as permissões para usuários e funções do IAM em contas-membro, incluindo o usuário-raiz da conta-membro. Qualquer conta tem somente as permissões permitidas por cada pai acima dela. Se uma permissão for bloqueada em qualquer nível acima da conta, implicitamente (sem ser incluída em uma declaração de política `Allow`) ou explicitamente (estar incluída em uma declaração de política `Deny`), o usuário ou a função na conta afetada não poderá usar essa permissão, mesmo que o administrador da conta anexe a política do IAM `AdministratorAccess` com permissões */* ao usuário.
- SCPs afetam apenas as contas-membro em sua organização. Eles não têm efeito sobre os usuários ou funções na conta de gerenciamento.
- Os usuários e funções ainda devem receber permissões com as políticas de permissão do IAM apropriadas. Um usuário sem nenhuma política de permissão do IAM não tem acesso, mesmo que as SCPs aplicáveis permitam todos os serviços e todas as ações.
- Se um usuário ou função tiver uma política de permissão do IAM que conceda acesso a uma ação que também é permitida pelas SCPs aplicáveis, o usuário ou a função poderá realizar essa ação.
- Se um usuário ou função tiver uma política de permissão do IAM que conceda acesso a uma ação que não é permitida ou é explicitamente negada pelas SCPs aplicáveis, o usuário ou a função não poderá executar essa ação.

- As SCPs afetam todos os usuários e funções em contas anexadas, incluindo o usuário raiz. As únicas exceções são aquelas descritas em Tarefas e entidades não restringidas por SCPs.
- As SCPs não afetam qualquer função vinculada ao serviço. As funções vinculadas a serviços permitem que outros AWS serviços se integrem AWS Organizations e não possam ser restringidos por SCPs.
- Quando você desabilita o tipo de política SCP em uma raiz, todos os SCPs são automaticamente separados de todas as AWS Organizations entidades nessa raiz. AWS Organizations as entidades incluem unidades organizacionais, organizações e contas. Se você ativar novamente as SCPs em uma raiz, essa raiz só será revertida para a política padrão `FullAWSAccess` automaticamente anexada a todas as entidades na raiz. Todos os anexos de SCPs a entidades do AWS Organizations anteriores à desabilitação de SCPs são perdidos e não são recuperáveis automaticamente, embora você possa reanexá-los manualmente.
- Se um limite de permissões (um recurso avançado do IAM) e uma SCP estiverem presentes, o limite, a SCP e a política baseada em identidade deverão permitir a ação.

## Uso de dados de acesso para melhorar as SCPs

Ao fazer login com as credenciais da conta de gerenciamento, você pode visualizar os dados do último acesso ao serviço para uma AWS Organizations entidade ou política na AWS Organizationsseção do console do IAM. Você também pode usar o AWS Command Line Interface (AWS CLI) ou a AWS API no IAM para recuperar os últimos dados acessados do serviço. Esses dados incluem informações sobre quais serviços permitidos os usuários e funções do IAM em uma AWS Organizations conta tentaram acessar pela última vez e quando. Você pode usar essas informações para identificar permissões não usadas, de forma que possa refinar suas SCPs para melhor aderir ao princípio de privilégio mínimo.

Por exemplo, você pode ter uma lista de negação SCP que proíba o acesso a três AWS serviços. Todos os serviços que não são listados na declaração `Deny` da SCP são permitidos. Os dados acessados pela última vez no IAM informam quais AWS serviços são permitidos pelo SCP, mas nunca são usados. Com essas informações, você pode atualizar a SCP para negar o acesso a serviços desnecessários.

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do IAM:

- Visualizar dados de serviços da organização acessados pela última vez para organizações
- Usar dados para refinar permissões de uma unidade organizacional

## Tarefas e entidades não restringidas por SCPs

Você não pode usar SCPs para restringir as seguintes tarefas:

- Qualquer ação executada pela conta de gerenciamento
- Qualquer ação executada usando permissões que são anexadas a uma função vinculada ao serviço
- Registrar-se no plano Enterprise Support como o usuário raiz
- Alterar o nível de AWS suporte como usuário root
- Forneça funcionalidade de assinante confiável para conteúdo CloudFront privado
- Configurar DNS reverso para um servidor de e-mail do Amazon Lightsail e uma instância do Amazon EC2 como o usuário-raiz
- Tarefas em alguns serviços AWS relacionados:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - API de marketing de produtos da Amazon

## Criar, atualizar e excluir de políticas de controle de serviço

Quando faz login na conta de gerenciamento da sua organização, você pode criar e atualizar políticas de controle de serviço (SCPs). Você cria SCPs gerando instruções que negam ou permitem o acesso a serviços e ações especificados.

A configuração padrão para trabalhar com SCPs é usar uma estratégia de "lista de bloqueios" em que todas as ações são implicitamente permitidas, exceto as ações que você deseja bloquear criando instruções que negam acesso. Com instruções de negação, você também pode especificar recursos e condições para a instrução e usar o elemento NotAction. Para instruções de permissão, você pode especificar apenas serviços e ações. Para obter mais informações sobre instruções que negam e permitem o acesso, consulte Avaliação do SCP.

> **Tip**
>
> Você pode usar os dados de serviços acessados mais recentemente no IAM como ponto de dados para atualizar suas SCPs para restringir o acesso a apenas os serviços da AWS

necessários. Para obter mais informações, consulte Visualizar os dados de serviço da organização acessados mais recentemente da organização no Guia do usuário do IAM.

Neste tópico:

- Depois de habilitar as políticas de controle de serviço para sua organização, você pode criar uma política.
- Quando os seus requisitos de SCP mudam, você pode atualizar uma política existente.
- Quando você não precisar mais de uma política e depois de desvinculá-la de todas as unidades organizacionais (UOs) e contas, você poderá excluí-la.

## Criar de uma SCP

**Permissões mínimas**

Para criar as SCPs, você precisa de permissão para executar a seguinte ação:

- `organizations:CreatePolicy`

AWS Management Console

Para criar uma política de controle de serviço

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Service control policies (Políticas de controle de serviço), escolha Create policy (Criar política).
3. Na página Create new service control policy (Criar nova política de controle de serviço), insira um nome de política e uma descrição da política opcional.
4. (Opcional) Adicione uma ou mais tags escolhendo Add tag (Adicionar tag) e inserindo uma chave e um valor opcional. Se deixar o valor em branco, ele é definido como uma sequência vazia, não `null`. É possível anexar até 50 tags a uma política. Para obter mais informações, consulte Marcando atributos AWS Organizations.

> **Note**
>
> Na maioria das etapas a seguir, discutimos o uso dos controles no lado direito do editor JSON para construir a política, elemento por elemento. Como alternativa, você pode, a qualquer momento, simplesmente inserir texto no editor JSON no lado esquerdo da janela. Você pode digitar diretamente, ou usar copiar e colar.

5. Para criar a política, suas próximas etapas variam, dependendo de se você deseja adicionar uma instrução que nega ou permite o acesso. Para obter mais informações, consulte Avaliação do SCP. Se você usar instruções `Deny`, você tem mais controle, pois pode restringir o acesso a recursos específicos, definir condições para quando as SCPs estão em vigor e usar o elemento NotAction. Para obter detalhes sobre sintaxe de, consulte Sintaxe de SCP.

   Para adicionar uma instrução que nega acesso:

   a. No painel direito Edit statement (Editar instrução) do editor, em Add actions (Adicionar ações), escolha um serviço da AWS.

      À medida que você escolher opções à direita, o editor JSON é atualizado para mostrar a política JSON correspondente à esquerda.

   b. Depois de selecionar um serviço, será aberta uma lista que contém as ações disponíveis para esse serviço. Você pode escolher All actions (Todas as ações) ou escolher uma ou mais ações individuais que você deseja negar.

      O JSON à esquerda é atualizado para incluir as ações selecionadas.

      > **Note**
      >
      > Se você selecionar uma ação individual e, em seguida, voltar e também selecionar All actions (Todas as ações), a entrada esperada para *`servicename`*`/*` é adicionada ao JSON, mas as ações individuais selecionadas anteriormente são deixadas no JSON e não são removidas.

   c. Se desejar adicionar ações de serviços adicionais, você pode escolher All services (Todos os serviços) na parte superior da caixa Statement (Instrução) e repetir as duas etapas anteriores, conforme necessário.

d. Especifique os recursos a serem incluídos na instrução.

- Ao lado de Add a resource (Adicionar um recurso), escolha Add (Adicionar).
- No diálogo Add resource (Adicionar recurso), escolha o serviço cujos recursos você deseja controlar na lista. Você pode selecionar apenas entre os serviços selecionados na etapa anterior.
- Em Resource type (Tipo de recurso), escolha o tipo de recurso que você deseja controlar.
- Finalmente, preencha o nome do recurso da Amazon (ARN) emResource ARN (ARN do recurso) para identificar o recurso específico ao qual você deseja controlar o acesso. Você deve substituir todos os espaços reservados que estão rodeados por chaves `{}`. Você pode especificar curingas (`*`) onde a sintaxe ARN desse tipo de recurso permitir. Consulte a documentação de um tipo de recurso específico para obter informações sobre onde você pode usar curingas.
- Salve sua adição à política escolhendo Add resource (Adicionar recurso). O elemento `Resource` no JSON reflete suas adições ou alterações. O elemento do recurso é necessário.

> **Tip**
>
> Se você desejar especificar todos os recursos para o serviço selecionado, escolha a opção All resources (Todos os recursos) na lista ou edite a instrução `Resource` diretamente no JSON para ler `"Resource":"*"`.

e. (Opcional) Para especificar condições que limitam quando uma instrução de política está em vigor, ao lado de Add condition (Adicionar condição), escolha Add (Adicionar).

- Condition key (Chave de condição) – a partir da lista, você pode escolher qualquer chave de condição disponível para todos os serviços AWS (por exemplo, `aws:SourceIp`) ou uma chave específica do serviço para apenas um dos serviços selecionados para esta instrução.
- Qualifier (Qualificador) – (opcional) se você inserir vários valores para a condição (dependendo da chave de condição especificada), poderá especificar um qualificador para testar solicitações para os valores.
  - Default (Padrão) – testa um único valor na solicitação em relação ao valor da chave de condição na política. A condição retornará true se o valor da chave na solicitação

corresponder ao valor na política. Se a política especificar mais de um valor, eles serão tratados como um teste "ou" e a condição retornará true se os valores da solicitação corresponderem a qualquer um dos valores de diretiva.

- For any value in a request (Para qualquer valor de uma solicitação) – quando a solicitação pode ter vários valores, esta opção testa se pelo menos um dos valores da solicitação corresponde a pelo menos um dos valores da chave de condição na política. A condição retorna verdadeiro se qualquer um dos valores de chave na solicitação corresponder a algum dos valores da condição na política. A condição retornará "falso" se nenhuma chave corresponder ou se houver um conjunto de dados nulo.
- For all values in a request (Para todos os valores em uma solicitação) – quando a solicitação pode ter vários valores, esta opção testa se todos os valores da solicitação correspondem ao valor da chave de condição na política. A condição retornará "verdadeiro" se cada valor de chave na solicitação corresponder a pelo menos um valor na política. Ela também retornará "verdadeiro" se não houver chaves na solicitação, ou se os valores de chave forem resolvidos para um conjunto de dados nulo, como uma string vazia.

- Operator (Operador) – o operador especifica o tipo de comparação a ser feita. As opções apresentadas dependem do tipo de dados da chave de condição. Por exemplo, a chave de condição global `aws:CurrentTime` permite que você escolha entre qualquer um dos operadores de comparação de datas, ou `Null`, que você pode usar para testar se o valor está presente na solicitação.

  Para qualquer operador de condição, exceto o teste `Null`, é possível escolher a opção IfExists.
- Value (Valor) – (opcional) especifique um ou mais valores para os quais você deseja testar a solicitação.

Escolha Add condition (Adicionar condição).

Para obter mais informações sobre o uso de chaves de condição, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.

f. (Opcional) para usar o elemento `NotAction` para negar acesso a todas as ações, exceto as especificadas, substitua `Action` por `NotAction` no painel à esquerda, logo após o elemento `"Effect": "Deny",`. Para obter mais informações, consulte Elementos da política JSON do IAM: ação no Guia do usuário do IAM.

6. Para adicionar uma instrução que permite acesso:

   a. No editor JSON à esquerda, altere a linha `"Effect": "Deny"` para `"Effect": "Allow"`.

      À medida que você escolher opções à direita, o editor JSON é atualizado para mostrar a política JSON correspondente à esquerda.

   b. Depois de selecionar um serviço, será aberta uma lista que contém as ações disponíveis para esse serviço. Você pode escolher All actions (Todas as ações) ou escolher uma ou mais ações individuais que você deseja permitir.

      O JSON à esquerda é atualizado para incluir as ações selecionadas.

      > **Note**
      >
      > Se você selecionar uma ação individual e, em seguida, voltar e também selecionar All actions (Todas as ações), a entrada esperada para *`servicename`*`/*` é adicionada ao JSON, mas as ações individuais selecionadas anteriormente são deixadas no JSON e não são removidas.

   c. Se desejar adicionar ações de serviços adicionais, você pode escolher All services (Todos os serviços) na parte superior da caixa Statement (Instrução) e repetir as duas etapas anteriores, conforme necessário.

7. (Opcional) Para adicionar outra instrução à política, escolha Add Statement (Adicionar instrução) e use o editor visual para criar a próxima instrução.

8. Ao concluir a adição de instruções, escolha Create policy (Criar política) para salvar a SCP concluída.

A nova SCP aparece na lista das políticas da organização. Agora você pode anexar a SCP à raiz, a UOs ou às contas.

AWS CLI & AWS SDKs

Para criar uma política de controle de serviço

Você pode usar um dos seguintes comandos para criar uma SCP:

- AWS CLI: create-policy

O exemplo a seguir pressupõe que você tenha um arquivo chamado `Deny-IAM.json` com o texto da política JSON nele. Ele usa esse arquivo para criar uma nova política de controle de serviço.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> As SCPs não entram em vigor na conta de gerenciamento e em algumas outras situações. Para obter mais informações, consulte Tarefas e entidades não restringidas por SCPs.

## Como atualizar uma SCP

Quando faz login na conta de gerenciamento da sua organização, você pode renomear ou alterar o conteúdo de uma política. A alteração do conteúdo de uma SCP afeta imediatamente todos os usuários, grupos e funções em todas as contas anexadas.

Permissões mínimas

Para atualizar uma SCP, você precisa de permissão para executar as seguintes ações:

- `organizations:UpdatePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política especificada (ou "*")
- `organizations:DescribePolicy` com um elemento `Resource` na mesma declaração de política que inclui o ARN da política especificada (ou "*")

AWS Management Console

Para atualizar uma política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Service control policies (Políticas de controle de serviço), escolha o nome da política que deseja atualizar.
3. Na página de detalhes da política, escolha Edit policy (Editar política).
4. Faça uma ou todas as alterações a seguir:
   - Você pode renomear a política inserindo um novo nome em Policy name (Nome da política).
   - Você pode alterar a descrição inserindo o novo texto em Policy description (Descrição da política).
   - Você pode editar o texto da política editando a política no formato JSON no painel esquerdo. Como alternativa, você pode escolher uma instrução no editor à direita e também alterar seus elementos usando os controles. Para obter mais detalhes sobre cada controle, consulte Criar um procedimento de SCP anteriormente neste tópico.
5. Ao concluir, escolha Save changes (Salvar alterações).

AWS CLI & AWS SDKs

Para atualizar uma política

Você pode usar um dos seguintes comandos para atualizar uma política:

- AWS CLI: update-policy

  O exemplo a seguir renomeia uma política.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

  O exemplo a seguir adiciona ou muda a descrição de uma política de controle de serviço.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
```

```
}
```

O exemplo a seguir altera o documento de política da SCP especificando um arquivo que contém o novo texto de política JSON.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

Para obter mais informações

Para obter mais informações sobre a criação de SCPs, consulte os seguintes tópicos:

- Exemplos de política de controle de serviço
- Sintaxe de SCP

## Edição de tags anexadas a uma SCP

Quando faz login na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a uma SCP. Para obter mais informações sobre marcação, consulte Marcando atributos AWS Organizations.

**Permissões mínimas**

Para editar as tags anexadas a uma SCP na sua organização da AWS, você deve ter as seguintes permissões:

- `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations
- `organizations:DescribePolicy` – necessária somente ao usar o console do Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

### AWS Management Console

Para editar de tags anexadas a uma SCP

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Service control policies (Políticas controle de serviços), escolha o nome da política com as etiquetas que você deseja editar.
3. Na página de detalhes da poítica, escolha a guia Tags (Etiquetas), depois escolha Manage tags (Gerenciar etiquetas).
4. Faça uma ou todas as alterações a seguir:
   - Edite o valor de uma etiqueta inserindo um novo valor sobre o antigo. Você não pode modificar diretamente a chave da etiqueta. Para alterar uma chave, você deve excluir a etiqueta com a chave antiga e adicionar uma tag com a nova chave.
   - Remova uma tag existente escolhendo Remove (Remover).
   - Adicione um novo par de chave e valor de tag. Escolha Add tag (Adicionar tag) e insira o novo nome da chave e o valor opcional nas caixas fornecidas. Se você deixar a caixa Value (Valor) vazia, o valor é uma sequência vazia, não é `null`.
5. Ao concluir, escolha Save changes (Salvar alterações).

AWS CLI & AWS SDKs

Para editar de tags anexadas a uma SCP

Você pode usar um dos seguintes comandos para alterar as tags anexadas a uma SCP:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

## Excluir uma SCP

Quando faz login na conta de gerenciamento da sua organização, você pode excluir uma política que não seja mais necessária em sua organização.

**Observações**

- Antes de excluir uma política, você deve primeiro desvinculá-la de todas as entidades anexadas.
- Você não pode excluir nenhuma SCP gerenciada pela AWS, como a SCP denominada `FullAWSAccess`.

**Permissões mínimas**

Para excluir uma SCP, você precisa de permissão para executar a seguinte ação:

- `organizations:DeletePolicy`

AWS Management Console

Para excluir uma SCP

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Service control policies (Políticas de controle de serviço), escolha o nome da SCP que você deseja excluir.

3. Você primeiro deve desvincular a política que deseja excluir de todas as raízes, UOs e contas. Escolha a guia Targets (Alvos), escolha o botão de opção ao lado de cada raiz, UO ou conta que é mostrada na lista Targets (Alvos) e escolha Detach (Desvincular). Na caixa de diálogo de confirmação, escolha Detach (Desvincular). Repita até remover todos os alvos.
4. Escolha Delete (Excluir), no alto da página.
5. Na caixa de diálogo de confirmação, insira o nome da política e escolha Delete (Excluir).

AWS CLI & AWS SDKs

Para excluir uma SCP

Você pode usar um dos seguintes comandos para excluir uma política:

- AWS CLI: delete-policy

  O exemplo a seguir exclui a SCP especificada.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: DeletePolicy

## Anexar e desvincular políticas de controle de serviço

Quando faz login na conta de gerenciamento da sua organização, você pode anexar uma política de controle de serviço (SCP) criada anteriormente. Você pode anexar uma SCP à raiz da organização, a uma unidade organizacional (UO) ou diretamente a uma conta. Para anexar uma SCP, conclua as seguintes etapas.

> **Permissões mínimas**
>
> Para anexar uma SCP a uma raiz, UO ou conta, você precisa de permissão para executar a seguinte ação:

- `organizations:AttachPolicy` com um elemento `Resource` na mesma instrução de política que inclui "*" ou o nome do recurso da Amazon (ARN) da política especificada e o ARN da raiz, UO ou conta que você deseja anexar à política

AWS Management Console

Você pode anexar uma SCP navegando até a política ou até a raiz, UO ou conta à qual você deseja anexar a política.

Para anexar uma SCP navegando para a raiz, UO ou conta

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue e marque a caixa de seleção ao lado da raiz, UO ou conta à qual você deseja anexar uma SCP. Talvez seja necessário expandir as UOs (escolha ▸) para encontrar a UO ou a conta que você deseja.
3. Na guia Policies (Políticas), na entrada para Service control policies (Políticas de controle de serviço), escolha Attach (Anexar).
4. Encontre a política que você deseja e escolha Attach policy (Anexar política).

   A lista de SCPs anexadas na guia Policies (Políticas) é atualizada para incluir a nova adição. A alteração da política tem efeito imediatamente, afetanto as permissões de usuários e funções do IAM na conta anexada ou em todas as contas na raiz ou UO anexada.

Para anexar uma SCP navegando até a política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Service control policies (Políticas de controle de serviço), escolha o nome da política que você deseja anexar.
3. Na guia Targets (Alvos), selecione Attach (Anexar).

4. Escolha o botão de opção ao lado da raiz, UO ou conta à qual você deseja anexar a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
5. Escolha Attach policy (Anexar política).

   A lista de SCPs anexadas na guia Targets (Alvos) é atualizada para incluir a nova adição. A alteração da política tem efeito imediatamente, afetando as permissões de usuários e funções do IAM na conta anexada ou em todas as contas na raiz ou UO anexada.

AWS CLI & AWS SDKs

Para anexar uma SCP navegando para a raiz, UO ou conta

Você pode usar um dos seguintes comandos para anexar uma SCP:

- AWS CLI: attach-policy

  O exemplo a seguir anexa uma SCP a uma UO.

```
$ aws organizations attach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS SDKs: AttachPolicy

A alteração da política tem efeito imediatamente, afetando as permissões de usuários e funções do IAM na conta anexada ou em todas as contas na raiz ou UO anexada.

## Desanexar uma SCP da raiz da organização, UO ou conta

Quando faz login na conta de gerenciamento de sua organização, você pode desvincular uma SCP da raiz da organização, UO ou conta à qual ela está anexada. Depois de separar um SCP de uma entidade, esse SCP não se aplica mais a nenhum usuário e função do IAM que tenha sido afetado pela entidade agora desanexada. Para desanexar uma SCP, conclua as seguintes etapas.

> **Note**
>
> Não é possível desanexar a última SCP de uma raiz, uma UO ou uma conta. Deve haver pelo menos uma SCP anexada a cada raiz, UO e conta durante todo o tempo.

> **Permissões mínimas**
>
> Para desvincular uma SCP da raiz, UO ou conta, você precisa de permissão para executar a seguinte ação:
>
> - `organizations:DetachPolicy`

AWS Management Console

Você pode desvincular uma SCP navegando até a política ou até a raiz, UO ou conta da qual você deseja desvincular a política.

Para desvincular uma SCP navegando até a raiz, UO ou conta à qual ela está anexada

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue até a raiz, UO ou conta da qual você deseja desvincular uma política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja. Escolha o nome da raiz, UO ou conta.
3. Na guia Policies (Políticas), escolha o botão de opção ao lado da SCP que você deseja desvincular e selecione Detach (Desvincular).
4. Na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

   A lista de SCPs anexadas será atualizada. A alteração da política causada pela desvinculação da SCP entra em vigor imediatamente. Por exemplo, a desvinculação de uma SCP afeta imediatamente as permissões de usuários e funções do IAM na conta anexada anteriormente ou contas abaixo da raiz ou UO anexada anteriormente.

Para desvincular uma SCP navegando até a política

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Service control policies (Políticas de controle de serviço), escolha o nome da política que você deseja desvincular de uma raiz, UO ou conta.
3. Na guia Targets (Alvos), escolha o botão de opção ao lado da raiz, UO ou conta da qual você deseja desvincular a política. Talvez seja necessário expandir as UOs (escolha ▶ ) para encontrar a UO ou a conta que você deseja.
4. Escolha Detach (Desvincular).
5. Na caixa de diálogo de confirmação, escolha Detach (Desvincular).

   A lista de SCPs anexadas será atualizada. A alteração da política causada pela desvinculação da SCP entra em vigor imediatamente. Por exemplo, a desvinculação de uma SCP afeta imediatamente as permissões de usuários e funções do IAM na conta anexada anteriormente ou contas abaixo da raiz ou UO anexada anteriormente.

AWS CLI & AWS SDKs

Para desvincular uma SCP de uma raiz, UO ou conta

Você pode usar um dos seguintes comandos para desvincular uma SCP:

- AWS CLI: detach-policy

  O exemplo a seguir desvincula a SCP especificada da UO especificada.

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWS SDKs: DetachPolicy

A alteração da política tem efeito imediatamente, afetando as permissões de usuários e funções do IAM na conta anexada ou em todas as contas na raiz ou UO anexada

# Avaliação do SCP

> **Note**
>
> As informações nesta seção não se aplicam a tipos de política de gerenciamento, incluindo políticas de exclusão dos serviços de IA, políticas de backup ou políticas de tag. Para obter mais informações, consulte Entendendo a herança da política de gerenciamento.

Como você pode anexar diversas políticas de controle de serviço (SCPs) em diferentes níveis no AWS Organizations, entender como as SCPs são avaliadas pode ajudá-lo a escrever SCPs que produzam o resultado correto.

Tópicos



## Como os SCPs funcionam com o Allow

Para que uma permissão seja concedida para uma conta específica, deve haver uma **`Allow`** declaração explícita em cada nível, desde a raiz até cada UO, no caminho direto até a conta (incluindo a própria conta de destino). É por isso que, quando você habilita SCPs, AWS Organizations anexa uma política de SCP AWS gerenciada chamada FullawsAccess que permite todos os serviços e ações. Se esta política for removida e não substituída em qualquer nível da organização, todas as UOs e contas nesse nível serão impedidas de realizar quaisquer ações.

Por exemplo, vamos examinar o cenário mostrado nas figuras 1 e 2. Para que uma permissão ou serviço seja permitido na Conta B, um SCP que permite a permissão ou serviço deve ser anexado à Raiz, à UO de Produção e à própria Conta B.

A avaliação de SCP segue um modelo de negação por padrão, o que significa que quaisquer permissões não explicitamente permitidas nos SCPs são negadas. Se uma instrução de permissão não estiver presente nas SCPs em nenhum dos níveis, como Raiz, UO de Produção ou Conta B, o acesso será negado.

Observações

- Uma instrução `Allow` em um SCP permite que o elemento `Resource` tenha apenas uma entrada `"*"`.
- Uma instrução `Allow` em uma SCP não pode ter um elemento `Condition`.

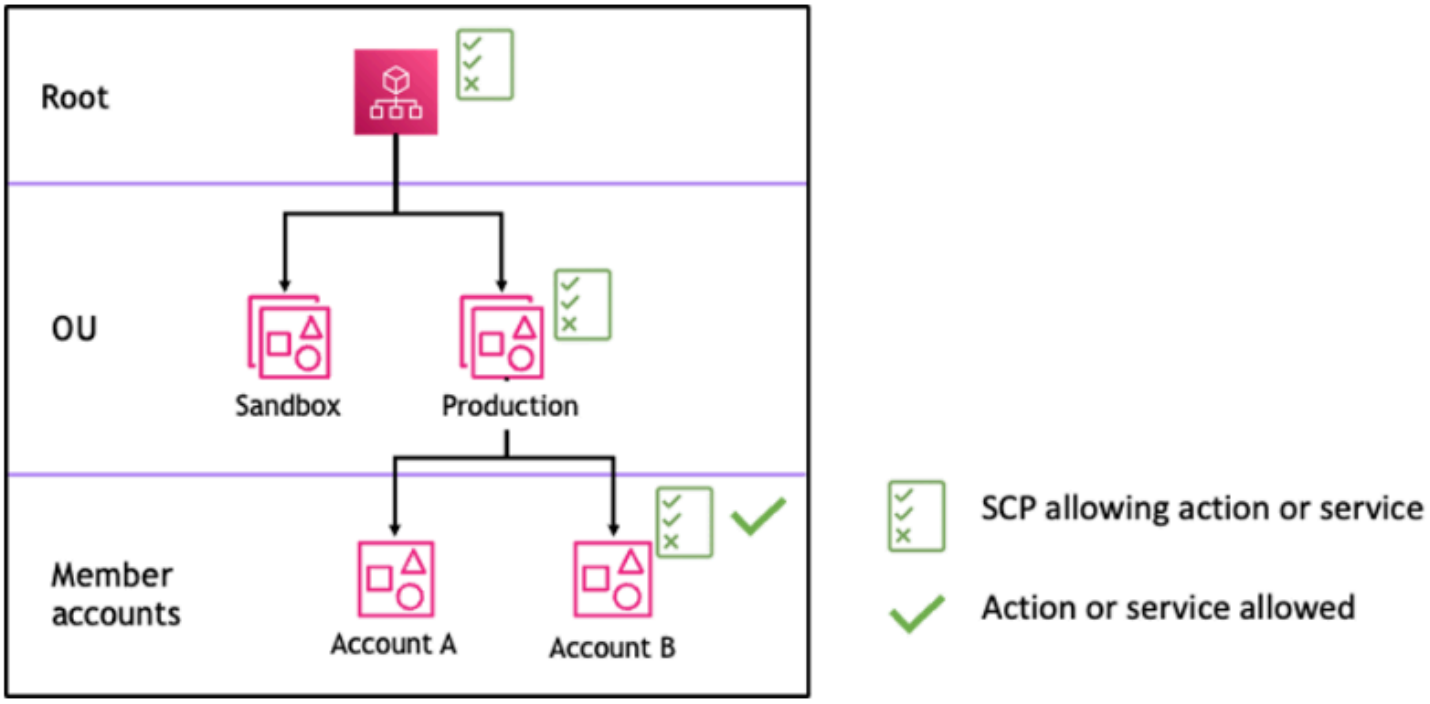



Figura 1: exemplo de estrutura organizacional com uma declaração *`Allow`* anexada na Raiz, UO de Produção e Conta B

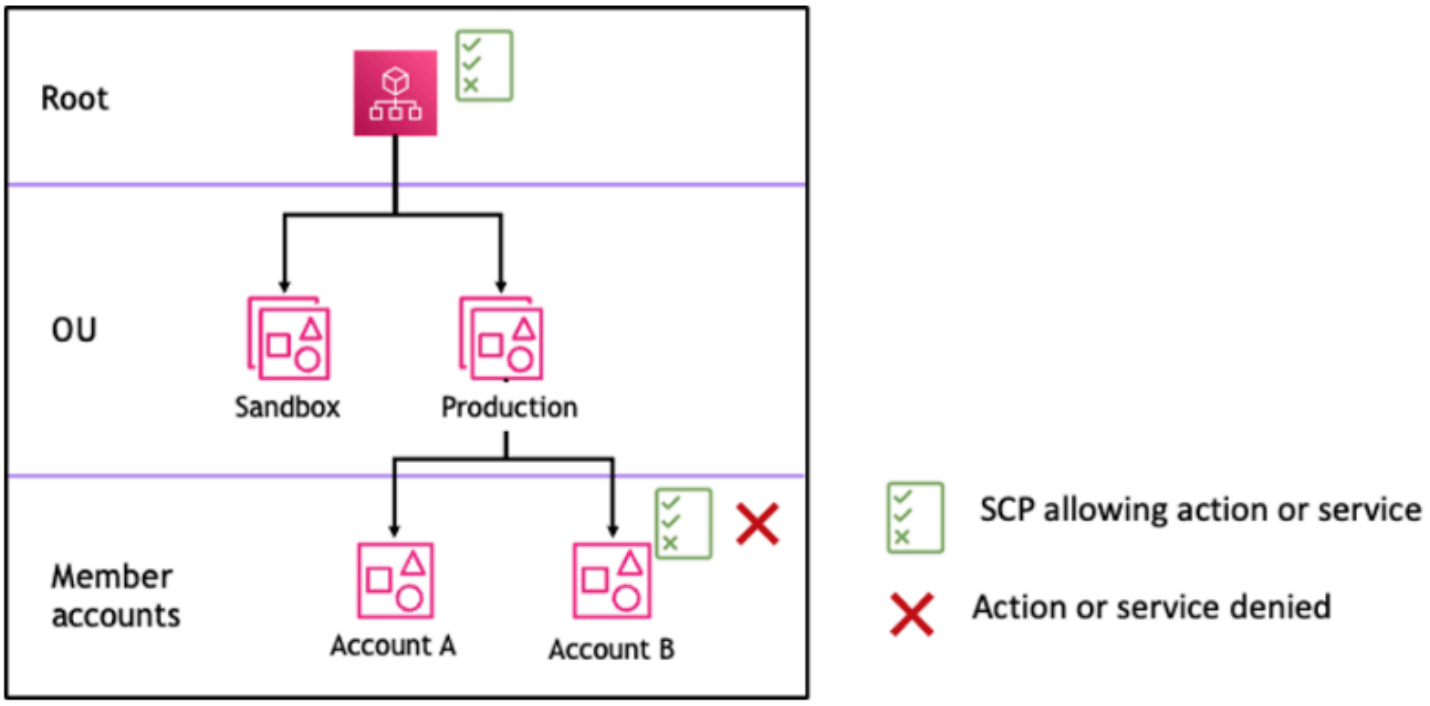



Figura 2: exemplo de estrutura organizacional com uma declaração *`Allow`* faltando na UO de Produção e seu impacto na Conta B

## Como os SCPs trabalham com negação

Para que uma permissão seja negada para uma conta específica, qualquer SCP da raiz até cada UO no caminho direto para a conta (incluindo a própria conta de destino) pode negar essa permissão.

Por exemplo, digamos que haja um SCP anexado à UO de Produção que tenha uma declaração `Deny` explícita especificada para um determinado serviço. Também há outro SCP conectado à raiz e à conta B que permite explicitamente o acesso ao mesmo serviço, conforme mostrado na Figura 3. Como resultado, tanto a Conta A quanto a Conta B terão acesso negado ao serviço, pois uma política de negação vinculada a qualquer nível da organização é avaliada para todas as UOs e contas de membros abaixo dela.

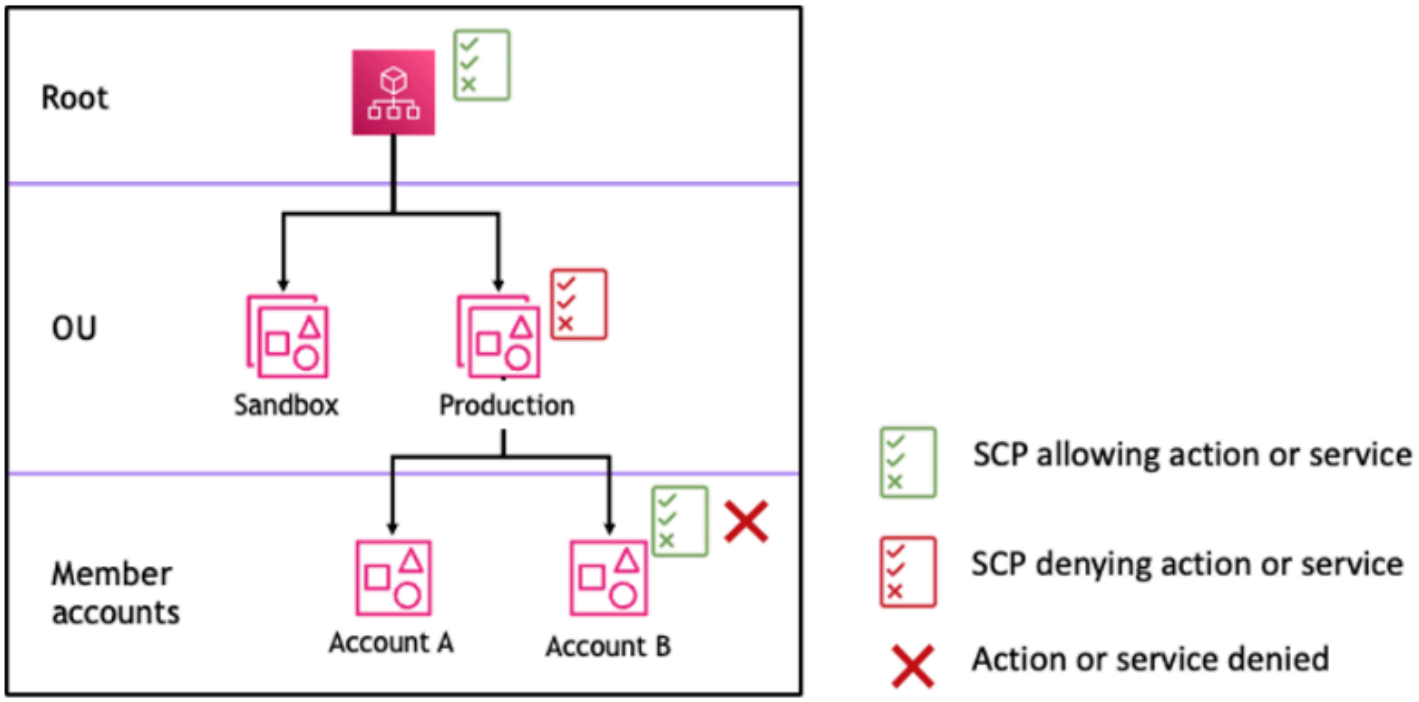



Figura 3: exemplo de estrutura organizacional com uma declaração *Deny* anexada na UO de Produção e seu impacto na Conta B

## Estratégias de uso de SCPs

Ao escrever SCPs, você pode usar uma combinação de `Allow` `Deny` declarações para permitir ações e serviços pretendidos em sua organização. As declarações `Deny` são uma forma poderosa de implementar restrições que devem ser verdadeiras para uma parte mais ampla de sua organização ou UOs porque, quando aplicadas na raiz ou no nível da UO, elas afetam todas as contas abaixo dela.

Por exemplo, você pode implementar uma política usando [Impedir que a conta membro saia da organização](#) no nível raiz, que será efetiva para todas as contas da organização. As instruções de negação também suportam o elemento de condição que pode ser útil para criar exceções.

> **Tip**
>
> Você pode usar os [dados de serviços acessados mais recentemente](#) no [IAM](#) para atualizar suas SCPs para restringir o acesso a apenas os serviços da AWS necessários. Para obter mais informações, consulte [Visualizar dados de serviço da organização acessados mais recentemente da organização](#) no Guia do usuário do IAM.

O AWS Organizations anexa um SCP gerenciado pelo AWS chamado FullAWSAccess a cada raiz, UO e conta quando ele é criado. Esta política permite todos os serviços e ações. Você pode substituir FullAWSAccess por uma política que permita apenas um conjunto de serviços para que novos serviços AWS não sejam permitidos, a menos que sejam explicitamente permitidos pela atualização de SCPs. Por exemplo, se a sua organização quiser permitir apenas o uso de um subconjunto de serviços no seu ambiente, você poderá usar uma declaração `Allow` para permitir apenas serviços específicos.

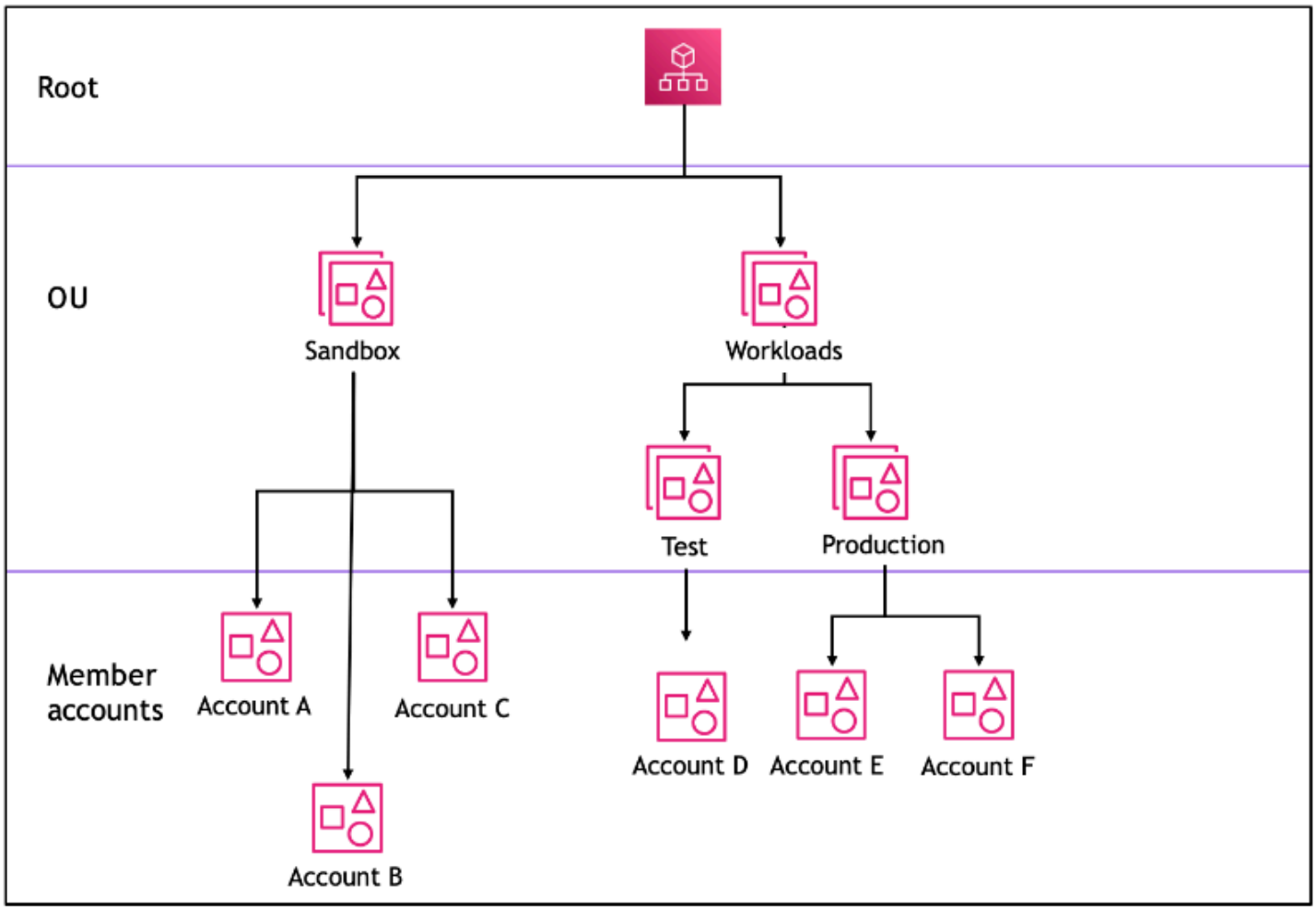
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Uma política que combina as duas declarações pode ser semelhante ao exemplo a seguir, que impede que contas-membro deixem a organização e permite o uso dos serviços AWS desejados. O administrador da organização pode desanexar a política FullAWSAccess e anexar essa no lugar.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
```

```
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Agora, considere o seguinte exemplo de estrutura organizacional para entender como você pode aplicar vários SCPs em diferentes níveis em uma organização.




A tabela a seguir mostra as políticas efetivas na UO de Sandbox.

| Cenário | SCP na Raiz | SCP na UO de Sandbox | SCP na Conta A | Política resultante na Conta A | Política resultante na Conta B e na Conta C |
|---|---|---|---|---|---|
| 1 | Acesso total AWS | Acesso AWS total + negar acesso ao S3 | Acesso AWS total + negar acesso ao EC2 | Sem acesso ao S3 e EC2 | Sem acesso ao S3 |
| 2 | Acesso total AWS | Permitir acesso ao Amazon Elastic Compute Cloud (Amazon EC2) | Permitir acesso ao EC2 | Permite acesso somente ao EC2 | Permite acesso somente ao EC2 |
| 3 | Negar acesso ao S3 | Permitir acesso ao S3 | Acesso total AWS | Sem acesso ao serviço | Sem acesso ao serviço |

A tabela a seguir mostra as políticas efetivas na UO de Workloads.

| Cenário | SCP na Raiz | SCP na UO de Workloads | SCP na UO de Teste | Política resultante na Conta D | Políticas resultantes na OU de Produção, na Conta E e Conta F |
|---|---|---|---|---|---|
| 1 | Acesso total AWS | Acesso total AWS | Acesso AWS total + negar acesso ao EC2 | Sem acesso ao EC2 | Acesso total AWS |

| Cenário | SCP na Raiz | SCP na UO de Workloads | SCP na UO de Teste | Política resultante na Conta D | Políticas resultantes na OU de Produção, na Conta E e Conta F |
|---|---|---|---|---|---|
| 2 | Acesso total AWS | Acesso total AWS | Permitir acesso ao EC2 | Permitir acesso ao EC2 | Acesso total AWS |
| 3 | Negar acesso ao S3 | Acesso total AWS | Permitir acesso ao S3 | Sem acesso ao serviço | Sem acesso ao serviço |

## Sintaxe de SCP

As políticas de controle de serviços (SCPs) usam uma sintaxe semelhante à usada pelas políticas de permissão AWS Identity and Access Management (IAM) e políticas baseadas em recursos (como as políticas de bucket do Amazon S3). Para obter mais informações sobre as políticas do IAM e sua sintaxe, consulte Visão geral das políticas do IAM no Guia do usuário do IAM.

Uma SCP é um arquivo de texto sem formatação estruturado de acordo com as regras do JSON. Ela usa os elementos que são descritos neste tópico.

> **Note**
>
> Todos os caracteres em sua conta de SCP contam em relação ao seu tamanho máximo. Os exemplos deste guia mostram as SCPs formatadas com espaço em branco adicional para melhorar a legibilidade. No entanto, para economizar espaço quando o tamanho da política se aproximar do tamanho máximo, é possível excluir todos os espaços em branco, como caracteres de espaço e quebras de linhas, que estiverem fora das aspas.

Para obter informações gerais sobre SCPs, consulte Políticas de controle de serviço (SCPs).

## Resumo de elementos

A seguinte tabela resume os elementos de políticas que você pode usar em SCPs. Alguns elementos de políticas estão disponíveis apenas em SCPs que negam ações. A coluna Supported effects (Efeitos com suporte) lista o tipo de efeito que você pode usar com cada elemento de política em SCPs.

| Elemento | Finalidade | Efeitos com suporte |
| --- | --- | --- |
| Version (Versão) | Especifica as regras da sintaxe da linguagem a serem usadas para processar a política. | `Allow`, `Deny` |
| Instrução | Serve como o contêiner para elementos de políticas. Você pode ter várias instruções em SCPs. | `Allow`, `Deny` |
| ID da instrução (Sid) | (Opcional) Fornece um nome amigável | `Allow`, `Deny` |

| Elemento | Finalidade | Efeitos com suporte |
| --- | --- | --- |
| | para a instrução. | |
| Efeito | Define se a instrução da SCP permite ou nega o acesso principal a usuários e funções do IAM em uma conta. | `Allow`, `Deny` |
| Ação | Especifica o AWS serviço e as ações que o SCP permite ou nega. | `Allow`, `Deny` |

| Elemento | Finalidade | Efeitos com suporte |
| --- | --- | --- |
| NotAction | Especifica a AWS serviços e ações que estão isentos do SCP. Usado em vez do elemento `Action`. | `Deny` |
| Recurso | Especifica a os AWS recursos aos quais o SCP se aplica. | `Deny` |
| Condição | Especifica a as condições em que a instrução está em vigor. | `Deny` |

As seguintes seções oferecem mais informações e exemplos de como os elementos de políticas são usados em SCPs.

## Elemento **`Version`**

Cada SCP deve incluir um elemento `Version` com o valor `"2012-10-17"`. Este é o mesmo valor da versão mais recente das políticas de permissão do IAM.

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

Para obter mais informações, consulte Elementos de política JSON do IAM: versão no Guia do usuário do IAM.

## Elemento **`Statement`**

Uma SCP consiste em um ou mais elementos `Statement`. Você pode ter apenas uma palavra-chave `Statement` em uma política, mas o valor pode ser uma matriz JSON de instruções (entre os caracteres []).

O exemplo a seguir mostra uma única instrução que consiste em elementos `Effect`, `Action` e `Resource` únicos.

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

O exemplo a seguir inclui duas instruções como uma lista de matrizes dentro de um elemento `Statement`. A primeira instrução permite todas as ações, enquanto a segunda nega todas as ações do EC2. O resultado é que um administrador da conta pode delegar qualquer permissão, exceto as do Amazon Elastic Compute Cloud (Amazon EC2).

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

Para obter mais informações, consulte Elementos de política JSON do IAM: instrução no Guia do usuário do IAM.

## Elemento ID da instrução (**`Sid`**)

O `Sid` é um identificador opcional que você fornece para a instrução da política. Você pode atribuir um valor `Sid` a cada instrução em uma matriz de instruções. A seguinte SCP de exemplo mostra uma instrução `Sid`.

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

Para obter mais informações, consulte Elementos de política JSON do IAM: Id no Guia do usuário do IAM.

## Elemento **`Effect`**

Cada instrução deve conter um elemento `Effect`. O valor pode ser `Allow` ou `Deny`. Isso afeta todas as ações listadas na mesma instrução.

Para obter mais informações, consulte Elementos de política JSON do IAM: efeito no Guia do usuário do IAM.

### **`"Effect": "Allow"`**

O seguinte exemplo mostra uma SCP com uma instrução que contém um elemento `Effect` com um valor de `Allow` que permite que os usuários da conta executem ações para o serviço Amazon S3. Esse exemplo é útil em uma organização que usa a estratégia de lista de permissões (em que todas as políticas de `FullAWSAccess` padrão são desvinculadas para que as permissões sejam implicitamente negadas por padrão). O resultado é que a instrução permite as permissões do Amazon S3 para todas as contas anexadas:

```
{
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
```

```
}
```

Embora ele use a mesma palavra-chave de valor `Allow` como uma política de permissões do IAM, em uma SCP, ele na realidade não concede permissões a um usuário para fazer alguma coisa. Em vez disso, os SCPs atuam como filtros que especificam as permissões máximas para os usuários do IAM e as funções do IAM em uma organização. No exemplo anterior, mesmo que um usuário na conta tivesse a política gerenciada `AdministratorAccess` anexada, a SCP limitaria todos os usuários na conta para apenas ações do Amazon S3.

### `"Effect": "Deny"`

Em uma instrução em que o elemento `Effect` tem um valor de `Deny`, você também pode restringir o acesso a recursos específicos ou definir condições para quando SCPs estiverem em vigor.

A seguinte tabela mostra um exemplo de como usar uma chave de condição em uma instrução de negação.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

Essa instrução em uma SCP define uma proteção para impedir que as contas afetadas (em que a SCP é anexada à própria conta ou à raiz ou UO da organização que contém a conta) executem instâncias do Amazon EC2 se a instância do Amazon EC2 não estiver definida como `t2.micro`. Mesmo que uma política do IAM que permite essa ação seja anexada à conta, a proteção criada pela SCP impedirá isso.

## Elementos **`Action`** e **`NotAction`**

Cada instrução deve conter um dos seguintes:

- Em instruções de permissão ou de negação, um elemento `Action`.
- Em instruções de negação apenas (em que o valor do elemento `Effect` é `Deny`), um elemento `Action` ou `NotAction`.

O valor do `NotAction` elemento `Action` or é uma lista (uma matriz JSON) de cadeias de caracteres que identificam AWS serviços e ações que são permitidos ou negados pela instrução.

Cada string consiste na abreviação do serviço (como "s3", "ec2", "iam" ou "organizations"), tudo em letras minúsculas, seguida por um ponto e vírgula e uma ação desse serviço. As ações e não ações diferenciam maiúsculas de minúsculas e devem ser digitadas conforme mostrado na documentação de cada serviço. Em geral, todas elas são digitadas com cada palavra começando com uma letra maiúscula e o restante em minúsculas. Por exemplo: `"s3:ListAllMyBuckets"`.

Você também pode usar caracteres curinga, como asterisco (*) ou ponto de interrogação (?) em uma SCP:

- Você também pode usar um asterisco como um curinga para corresponder a várias ações que compartilham parte de um nome. O valor `"s3:*"` significa todas as ações no serviço Amazon S3. O valor de `"ec2:Describe*"` corresponde apenas às ações do EC2 que começam com "Describe".
- Use o curinga ponto de interrogação (?) para corresponder a um único caractere.

> **Note**
>
> Em uma SCP, os caracteres curinga (*) e (?) em um elemento `Action` ou `NotAction` só pode ser usado sozinho ou no final da string. Ele não pode aparecer no início nem no meio da string. Portanto, `"servicename:action*"` é válido, mas `"servicename:*action"` e `"servicename:some*action"` são inválidos em SCPs.

Para obter uma lista de todos os serviços e ações que eles suportam nas políticas de permissão do IAM e das AWS Organizations SCPs, consulte Ações, recursos e chaves de condição para AWS serviços no Guia do usuário do IAM.

Para obter mais informações, consulte Elementos de política JSON do IAM: ação e Elementos da política JSON do IAM: NotAction no Guia do usuário do IAM.

### Exemplo do elemento **`Action`**

O seguinte exemplo mostra uma SCP com uma instrução que permite que os administradores de contas deleguem permissões para descrever, iniciar, interromper e encerrar a instâncias do EC2 na conta. Este é um exemplo de uma lista de permissões e é útil quando as políticas `Allow *` padrão não são anexadas, para que, por padrão, as permissões sejam implicitamente negadas. Se a política `Allow *` padrão ainda estiver anexada à raiz, à UO ou à conta à qual a política a seguir está anexada, a política não terá efeito.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

O exemplo a seguir mostra como é possível negar o acesso a serviços que você não deseja que sejam usados em contas anexadas. Ele pressupõe que as SCPs `"Allow *"` padrão ainda estejam anexadas a todas as UOs e à raiz. Esse exemplo de política impede que os administradores de contas anexadas deleguem permissões para os serviços IAM, Amazon EC2 e Amazon RDS . Qualquer ação de outros serviços pode ser delegada, desde que não haja outra política anexada que a negue.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

Exemplo do elemento **`NotAction`**

O exemplo a seguir mostra como você pode usar um `NotAction` elemento para excluir AWS serviços do efeito da política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
       }
     }
   ]
}
```

Com essa declaração, as contas afetadas estão limitadas a realizar ações no especificado Região da AWS, exceto ao usar ações do IAM.

## Elemento **`Resource`**

Em instruções em que o elemento `Effect` tem um valor de `Allow`, você pode especificar apenas "*" no elemento `Resource` de uma SCP. Você não pode especificar nomes de recursos da Amazon (ARNs) individuais.

Você também pode usar caracteres curinga, como asterisco (*) ou ponto de interrogação (?) no elemento de recurso:

- Você também pode usar um asterisco como um curinga para corresponder a várias ações que compartilham parte de um nome.
- Use o curinga ponto de interrogação (?) para corresponder a um único caractere.

Em instruções em que o elemento `Effect` tem um valor de `Deny`, você pode especificar ARNs individuais, conforme mostrado no seguinte exemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

Esta SCP restringe que as entidades principais do IAM em contas façam alterações em uma função administrativa comum do IAM criada em todas as contas em sua organização.

Para obter mais informações, consulte Elementos da política JSON do IAM: recurso no Guia do usuário do IAM.

## Elemento **`Condition`**

Você pode especificar um elemento `Condition` em instruções de negação em uma SCP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
```

```
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

Esta SCP nega acesso a todas as operações fora das regiões `eu-central-1` e `eu-west-1`, exceto para ações nos serviços listados.

Para obter mais informações, consulte IAM JSON Policy Elements: Condition (Elementos da política JSON do IAM: Condição) no Guia do usuário do IAM.

### Elementos sem suporte

Os seguintes elementos não são compatíveis em SCPs:

- `Principal`
- `NotPrincipal`
- `NotResource`

## Exemplos de política de controle de serviço

O exemplo de políticas de controle de serviço (SCPs) exibido neste tópico tem finalidade apenas informativa.

> **Antes de usar esses exemplos**
>
> Antes de usar esses exemplos de SCPs em sua organização, faça o seguinte:

- Revise atentamente e personalize os SCPs de acordo com suas necessidades específicas.
- Teste detalhadamente os SCPs em seu ambiente com os serviços AWS que você usa.

  Os exemplos de políticas nesta seção demonstram a implementação e o uso de SCPs. Eles não são destinados a ser interpretado como recomendações oficiais ou práticas recomendadas da AWS a serem implementadas exatamente como mostrado. É sua responsabilidade testar cuidadosamente quaisquer políticas baseadas em negação quanto à sua adequação para resolver os requisitos de negócios do seu ambiente. As políticas de controle de serviço baseadas em negação podem limitar ou bloquear involuntariamente o uso de serviços da AWS, a menos que você adicione as exceções necessárias à política. Para obter um exemplo dessa exceção, consulte o primeiro exemplo que isenta os serviços globais das regras que bloqueiam o acesso a Regiões da AWS indesejadas.
- Lembre-se de que uma SCP afeta cada usuário e perfil, inclusive o usuário raiz, em cada conta à qual ela é anexada.

**Tip**

Você pode usar os dados de serviços acessados mais recentemente no IAM para atualizar suas SCPs para restringir o acesso a apenas os serviços da AWS necessários. Para obter mais informações, consulte Visualizar dados de serviço da organização acessados mais recentemente da organização no Guia do usuário do IAM.

Todas as políticas a seguir são um exemplo de uma estratégia de política de lista de negações. As políticas da lista de negações devem ser anexadas a outras políticas que permitam as ações aprovadas nas contas afetadas. Por exemplo, a política padrão `FullAWSAccess` permite o uso de todos os serviços em uma conta. Essa política é anexada por padrão na raiz, em todas as unidades organizacionais (UOs) e em todas as contas. Na verdade, não concede as permissões; nenhuma SCP faz isso. Em vez disso, ela permite que os administradores nessa conta deleguem acesso a essas ações anexando políticas de permissão padrão do AWS Identity and Access Management (IAM) a usuários, funções ou grupos na conta. Todas essas políticas de lista de negações substituem qualquer política bloqueando o acesso a serviços ou ações especificados.

Exemplos

- Exemplos gerais

- Impedir os usuários de excluir logs de fluxo da Amazon VPC
- Impedir qualquer VPC, que ainda não tenha acesso à internet, de obtê-lo

## Exemplos gerais

Negar acesso a AWS com base na Região da AWS solicitada

Este SCP nega o acesso a quaisquer operações fora das regiões especificadas. Substituia `eu-central-1` e `eu-west-1` pelo Regiões da AWS que você deseja usar. Ele fornece isenções para operações em serviços globais aprovados. Este exemplo também mostra como isentar solicitações feitas por uma das duas funções de administrador especificadas.

> **Note**
>
> Para usar a Região deny SCP com AWS Control Tower, consulte Negar acesso a AWS com base na Região da AWS solicitada.

Essa política usa o efeito `Deny` para negar acesso a todas as solicitações de operações que não visam uma das duas regiões aprovadas (`eu-central-1` e `eu-west-1`). O elemento NotAction permite listar serviços cujas operações (ou operações individuais) estão isentas dessa restrição. Como os serviços globais têm endpoints fisicamente hospedados pela região `us-east-1`, eles devem ser isentados dessa maneira. Com um SCP estruturado dessa forma, as solicitações feitas aos serviços globais na região `us-east-1` serão permitidas se o serviço solicitado estiver incluído no elemento `NotAction`. Quaisquer outras solicitações para serviços na região `us-east-1` são negadas por essa política de exemplo.

> **Note**
>
> Este exemplo pode não incluir todos os últimos serviços ou operações globais da AWS. Substitua a lista de serviços e operações pelos serviços globais usados por contas em sua organização.
>
> > **Dica**
> >
> > É possível visualizar os dados do serviço acessados pela última vez no console do IAM para determinar quais serviços globais são usados pela sua organização. A guia Consultor de acesso na página de detalhes de um usuário, um grupo ou uma função

do IAM exibe os serviços da AWS que foram usados por essa entidade, classificados pelo acesso mais recente.

Considerações

- AWS KMS e AWS Certificate Manager suportam endpoints regionais. No entanto, se você quiser usá-los com um serviço global como o Amazon CloudFront, você deve incluí-los na lista de exclusão de serviço global na SCP do exemplo a seguir. Um serviço global como o Amazon CloudFront geralmente requer acesso ao AWS KMS e o ACM na mesma região, que para um serviço global é a região Leste dos EUA (Norte da Virgínia) (`us-east-1`).
- Por padrão, o AWS STS é um serviço global e deve ser incluído na lista global de exclusão de serviços. No entanto, você pode habilitar o AWS STS para usar endpoints de região em vez de um único endpoint global. Se você fizer isso, você pode remover STS da lista de isenção de serviço global na SCP do exemplo a seguir. Para obter mais informações, consulte Gerenciar o AWS STS no Região da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
```

```
            "ec2:DescribeTransitGateways",
            "ec2:DescribeVpnGateways",
            "fms:*",
            "globalaccelerator:*",
            "health:*",
            "iam:*",
            "importexport:*",
            "kms:*",
            "mobileanalytics:*",
            "networkmanager:*",
            "organizations:*",
            "pricing:*",
            "route53:*",
            "route53domains:*",
            "route53-recovery-cluster:*",
            "route53-recovery-control-config:*",
            "route53-recovery-readiness:*",
            "s3:GetAccountPublic*",
            "s3:ListAllMyBuckets",
            "s3:ListMultiRegionAccessPoints",
            "s3:PutAccountPublic*",
            "shield:*",
            "sts:*",
            "support:*",
            "trustedadvisor:*",
            "waf-regional:*",
            "waf:*",
            "wafv2:*",
            "wellarchitected:*"
        ],
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "aws:RequestedRegion": [
                    "eu-central-1",
                    "eu-west-1"
                ]
            },
            "ArnNotLike": {
                "aws:PrincipalARN": [
                    "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                    "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                ]
            }
```

```
            }
        }
    ]
}
```

Evite que usuários e funções do IAM façam determinadas alterações

Esta SCP restringe que usuários e funções do IAM façam alterações em uma função do IAM criada em todas as contas em sua organização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

Impedir que usuários e funções do IAM façam alterações especificadas, com uma exceção para uma função de administrador especificada

Esta SCP se baseia no exemplo anterior para fazer uma exceção para administradores. Isso impede que usuários e funções do IAM nas contas afetadas façam alterações em uma função administrativa comum do IAM criada em todas as contas em sua organização, exceto para os administradores que usam uma função especificada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

Exigir MFA para executar uma ação de API

Use uma SCP, como a seguinte, para exigir que a autenticação multifator (MFA) seja habilitada para que uma un usuário ou função do IAM possa executar uma ação. Neste exemplo, a ação é interromper uma instância do Amazon EC2.

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

```
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Bloquear o acesso ao serviço para o usuário root

A seguinte política restringe o acesso a ações especificadas para o usuário root em uma conta membro. Para impedir que suas contas usem credenciais raiz de formas específicas, adicione suas próprias ações a esta política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

Impedir que a conta membro saia da organização

A política a seguir bloqueia o uso da operação de API `LeaveOrganization` para que os administradores de contas membro não possam remover suas contas da organização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

## Exemplo de SCPs para o Amazon CloudWatch

Exemplos nesta categoria

- Impedir que os usuários desabilitem o CloudWatch ou alterem sua configuração

Impedir que os usuários desabilitem o CloudWatch ou alterem sua configuração

Um operador do CloudWatch de nível inferior precisa monitorar painéis e alarmes. No entanto, o operador não pode excluir ou alterar nenhum painel ou alerta que o pessoal sênior tenha implantado. Essa SCP impede que usuários ou funções em qualquer conta afetada executem qualquer um dos comandos do CloudWatch que podem excluir ou alterar seus painéis ou alarmes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

## Exemplo de SCPs para o AWS Config

Exemplos nesta categoria

- Impedir que os usuários desabilitem a AWS Config ou alterem suas regras

Impedir que os usuários desabilitem a AWS Config ou alterem suas regras

Essa SCP impede que usuários ou funções em qualquer conta afetada executem operações do AWS Config que possam desabilitar o AWS Config ou alterar suas regras ou triggers.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

## Exemplo de SCPs para Amazon Elastic Compute Cloud (Amazon EC2)

Exemplos nesta categoria

- Exigir que as instâncias do Amazon EC2 usem um tipo específico
- Evitar o lançamento de instâncias do EC2 sem o IMDSv2
- Evitar a desativação da criptografia padrão do Amazon EBS

Exigir que as instâncias do Amazon EC2 usem um tipo específico

Com esta SCP, qualquer instância executada que não usa o tipo de instância `t2.micro` é negada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

Evitar o lançamento de instâncias do EC2 sem o IMDSv2

A política a seguir impede que todos os usuários iniciem instâncias do EC2 sem o IMDSv2.

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
```

```
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

A política a seguir impede que todos os usuários iniciem instâncias do EC2 sem o IMDSv2, mas permite que identidades específicas do IAM modifiquem as opções de metadados da instância.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
```

```
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

Evitar a desativação da criptografia padrão do Amazon EBS

A política a seguir impede que todos os usuários desabilitem a criptografia padrão do Amazon EBS.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

## Exemplo de SCPs para o Amazon GuardDuty

Exemplos nesta categoria

- Impedir que os usuários desabilitem o GuardDuty ou modifiquem sua configuração

Impedir que os usuários desabilitem o GuardDuty ou modifiquem sua configuração

Essa SCP impede que usuários ou funções em qualquer conta afetada desabilitem o GuardDuty ou alterem sua configuração, diretamente como um comando ou por meio do console. Ela permite efetivamente o acesso somente leitura às informações e recursos do GuardDuty.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

## Exemplo de SCPs para o AWS Resource Access Manager

Exemplos nesta categoria

- Evitar compartilhamento externo
- Permitir que contas específicas compartilhem apenas tipos de recursos especificados
- Evitar o compartilhamento com organizações ou unidades organizacionais (UOs)
- Permitir o compartilhamento com apenas usuários e funções do IAM especificados

### Evitar compartilhamento externo

O exemplo a seguir, a SCP impede que os usuários criem compartilhamentos de recursos que permitem o compartilhamento com usuários e funções do IAM que não fazem parte da organização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Permitir que contas específicas compartilhem apenas tipos de recursos especificados

A SCP a seguir permite que contas 111111111111 e 222222222222 criem compartilhamentos de recursos que compartilham listas de prefixos e associar listas de prefixos a compartilhamentos de recursos existentes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

Evitar o compartilhamento com organizações ou unidades organizacionais (UOs)

A SCP a seguir impede que os usuários criem compartilhamentos de recursos que compartilham recursos com uma organização ou UOs do AWS.

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

```
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Permitir o compartilhamento com apenas usuários e funções do IAM especificados

O exemplo a seguir, a SCP permite que os usuários compartilhem recursos apenas com organização `o-12345abcdef`, unidade organizacional`ou-98765fedcba`, e conta `111111111111`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
```

```
        }
    ]
}
```

## Exemplos de SPCs para Amazon Route 53 Application Recovery Controller

Exemplos nesta categoria

- Impedir que os usuários atualizem os estados de controle de roteamento do Route 53 ARC

Impedir que os usuários atualizem os estados de controle de roteamento do Route 53 ARC

Um operador do Route 53 ARC de nível mais baixo precisa monitorar painéis e visualizar informações do Route 53 ARC. No entanto, o operador não deve ter permissão para atualizar controles de roteamento que permitam a ele realizar o fail over da aplicação de um Região da AWS para outro, ao contrário do que um operador sênior poderia ter permissão para fazer. Esta SCP impede que usuários ou perfis em qualquer conta afetada executem operações do Route 53 ARC que atualizam os controles de roteamento do Route 53 ARC.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

# Exemplos de SCPs para o Amazon S3

Exemplos nesta categoria

- Evitar o upload de objetos não criptografados do Amazon S3

## Evitar o upload de objetos não criptografados do Amazon S3

A política a seguir impede que todos os usuários façam upload de objetos não criptografados para buckets do S3.

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

A política a seguir restringe que todos os usuários façam upload de objetos não criptografados para buckets do S3 e também impõe um tipo de criptografia específico (AES256 ou aws:kms) para o upload de objetos em seus buckets.

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
```

```
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

## Exemplo de SCPs para marcação de recursos

Exemplos nesta categoria

- Exigir uma tag em recursos criados especificados
- Impedir que as tags sejam modificadas, exceto por principais autorizados

### Exigir uma tag em recursos criados especificados

A SCP a seguir impede que usuários e funções do IAM nas contas afetadas criem determinados tipos de recursos se a solicitação não incluir as tags especificadas.

> **Important**
>
> Lembre-se de testar políticas baseadas em negação com os serviços que você usa em seu ambiente. O exemplo a seguir é um simples bloco de criação de segredos sem tags ou execução de instâncias do Amazon EC2 sem tags, e não inclui exceções.
> A política de exemplo a seguir não é compatível com o AWS CloudFormation como escrito, porque esse serviço cria um segredo e, em seguida, o marca como duas etapas separadas. Este exemplo de política efetivamente bloqueia o AWS CloudFormation de criar um segredo como parte de uma pilha, porque tal ação resultaria, embora brevemente, em um segredo que não é marcado como necessário.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
```

```
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
```

```
  ]
}
```

Para obter uma lista de todos os serviços e ações aos quais oferecem suporte em SCPs do AWS Organizations e em políticas de permissões do IAM, consulte Ações, recursos e chaves de condições para serviços da AWS no Guia do usuário do IAM.

Impedir que as tags sejam modificadas, exceto por principais autorizados

A SCP a seguir mostra como uma política pode permitir que apenas principais autorizados modifiquem as tags anexadas aos seus recursos. Essa é uma parte importante do uso do controle de acesso baseado em atributo (ABAC) como parte da sua estratégia de segurança de nuvem do AWS. A política permite que um chamador modifique as tags somente nos recursos em que a tag de autorização (neste exemplo, `access-project`) corresponde exatamente à mesma tag de autorização anexada ao usuário ou à função que está fazendo a solicitação. A política também impede que o usuário autorizado altere o valor da tag que é usada para autorização. O principal de chamada deve ter a etoqueta de autorização para fazer qualquer alteração.

Esta política só impede que usuários não autorizados alterem tags. Um usuário autorizado que não está bloqueado por esta política ainda deve ter uma política do IAM separada que conceda explicitamente a permissão `Allow` nas APIs de marcação relevantes. Por exemplo, se o usuário tiver uma política de administrador com`Allow */*` (permitir todos os serviços e todas as operações), então a combinação resulta na permissão do usuário administrador para alterar apenas as tags que têm um valor de tag de autorização que corresponde ao valor de tag de autorização anexada ao principal do usuário. Isso ocorre porque o `Deny` explícito nesta política substitui o `Allow` explícito na política de administrador.

> **Important**
>
> Esta não é uma solução de política completa e não deve ser usada como mostrado aqui. Este exemplo destina-se apenas a ilustrar parte de uma estratégia de ABAC e precisa ser personalizado e testado para ambientes de produção.
> Para obter a política completa com uma análise detalhada de como ela funciona, consulte Protegendo tags de recursos usadas para autorização usando uma política de controle de serviço no AWS Organizations
> Lembre-se de testar políticas baseadas em negação com os serviços que você usa em seu ambiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
```

```
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

## Exemplo de SCPs para a Amazon Virtual Private Cloud (Amazon VPC)

Exemplos nesta categoria

- Impedir os usuários de excluir logs de fluxo da Amazon VPC
- Impedir qualquer VPC, que ainda não tenha acesso à internet, de obtê-lo

### Impedir os usuários de excluir logs de fluxo da Amazon VPC

Essa SCP impede que usuários ou funções em qualquer conta afetada excluam logs de fluxo do Amazon Elastic Compute Cloud (Amazon EC2) ou grupos de log ou streams de log do CloudWatch.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

Impedir qualquer VPC, que ainda não tenha acesso à internet, de obtê-lo

Essa SCP impede que usuários ou funções em qualquer conta afetada alterem a configuração nuvens privadas virtuais (VPCs) do Amazon EC2 para conceder acesso direto à internet. Ela não bloqueia o acesso direto existente nem qualquer acesso roteado por meio do ambiente de rede local.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

# Gerenciar unidades organizacionais

Você pode usar unidades organizacionais (UOs) para agrupar contas e administrá-las como uma unidade única. Isso simplifica bastante o gerenciamento de suas contas. Por exemplo, você pode anexar um controle baseado em política a uma UO, e todas as contas da UO herdarão a política automaticamente. Você pode criar várias UOs em uma única organização, e pode criar UOs dentro de outras UOs. Cada UO pode conter várias contas, e você pode mover contas de uma UO para outra. No entanto, os nomes da UO devem ser exclusivos em uma UO pai ou raiz.

> **Note**
>
> Há uma raiz na organização, que é AWS Organizations criada para você quando você configura sua organização pela primeira vez.

Tópicos



Você também pode revisar todas as unidades organizacionais em sua organização. Para obter mais informações, consulte Visualizar detalhes de uma unidade organizacional.

## Navegar a raiz e a hierarquia da UO

Para navegar para diferentes UOs ou para a raiz quando mover contas ou anexar políticas, você pode usar a visualização padrão em "árvore".

AWS Management Console

Para navegar na organização como uma "árvore"

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, na parte superior da seção Organization (Organização), selecione Hierarchy (Hierarquia) em vez de List (Lista).
3. A árvore é exibida inicialmente mostrando a raiz, com apenas o primeiro nível de UOs e contas subordinadas exibido. Para expandir a árvore para mostrar níveis mais profundos, escolha o ícone de expansão ( ) ao lado de qualquer entidade superior. Para reduzir a desorganização e recolher uma ramificação da árvore, escolha o ícone ( ) ao lado de uma entidade superior expandida.
4. Escolha o nome de uma UO ou raiz para exibir seus detalhes e executar determinadas operações. Como alternativa, você pode escolher o botão ao lado do nome e executar determinadas operações nessa entidade no menu Actions (Ações).

Você também pode exibir a lista apenas das contas de sua organização em formato tabular, sem precisar primeiro navegar para uma UO para encontrá-las. Nesta exibição, você não pode ver nenhuma UO nem manipular as políticas anexadas a elas.

AWS Management Console

Para exibir a organização como uma lista simples de contas sem hierarquia

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na Contas da AWSpágina, na parte superior da seção Organização, escolha o ícone do interruptor Exibir Contas da AWS somente para ativá-lo. .
3. A lista de contas é exibida sem qualquer hierarquia.

# Criar uma UO

Quando faz login na conta de gerenciamento de sua organização, você pode criar uma UO na raiz da organização. As UOs podem ser aninhadas em até cinco níveis de profundidade. Para criar uma UO, conclua as seguintes etapas.

**Important**

Se essa organização for gerenciada com AWS Control Tower, crie suas OUs com o AWS Control Tower console ou as APIs. Se você criar a OU em Organizations, essa OU não será registrada no AWS Control Tower. Para obter mais informações, consulte Referência a recursos fora do AWS Control Tower no Manual do usuário doAWS Control Tower .

**Permissões mínimas**

Para criar uma UO dentro de uma raiz em sua organização, você precisa ter as seguintes permissões:

- `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations
- `organizations:CreateOrganizationalUnit`

AWS Management Console

Para criar uma UO

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Navegue até o página Contas da AWS.

   O console exibe a UO-raiz e seu conteúdo. Na primeira vez em que você acessa uma raiz, o console exibe todas as suas Contas da AWS na visualização de nível superior. Se você criou s anteriormente e movimentou contas nelas, o console mostrará apenas as UOs de nível superior e as contas que ainda não foram movidas para uma UO.

3. (Opcional) Se você desejar criar uma UO dentro de uma UO existente, navegue até a UO subordinada escolhendo o nome (não a caixa de seleção) da UO subordinada, ou escolhendo o

ao lado das UOs na visualização em árvore até ver a que deseja e depois escolhendo seu nome.
4. Quando você tiver selecionado a UO superior correta na hierarquia, no menu Actions (Ações), em Organizational Unit (Unidade Organizacional), escolha Create new (Criar nova)
5. Na caixa de diálogo Create organizational unit (Criar unidade organizacional), insira o nome da UO que você deseja criar.
6. (Opcional) Adicione uma ou mais tags escolhendo Add tag (Adicionar tag) e inserindo uma chave e um valor opcional. Se deixar o valor em branco, ele é definido como uma sequência vazia, não `null`. É possível anexar até 50 tags a uma UO.
7. Por fim, selecione Create organizational unit (Criar unidade organizacional).

A nova UO aparece dentro do pai. Agora você pode mover contas para essa UO ou anexar políticas a ela.

AWS CLI & AWS SDKs

Para criar uma UO

Você pode usar um dos seguintes comandos para criar uma UO:

- AWS CLI: create-organizational-unit

  Para criar uma UO, primeiro é preciso localizar a identidade da raiz ou a UO que você deseja como superior da nova UO.

  Para encontrar a identidade da raiz, use o comando list-roots. Para localizar a identidade de uma UO, use o comando list-children para navegar até a UO desejada.

  O exemplo a seguir mostra como localizar a identidade da raiz e, em seguida, encontrar a identidade de uma UO sob a raiz. O último comando mostra como criar uma nova UO na UO encontrada.

```
$ aws organizations list-roots
{
    "Roots": [
```

```
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children \
    --parent-id r-a1b2 \
    --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- AWS SDKs: CreateOrganizationalUnit

# Renomear uma UO

Quando faz login na conta de gerenciamento de sua organização, você pode renomear uma UO. Para fazer isso, conclua as seguintes etapas.

> **Permissões mínimas**
>
> Para renomear uma OU dentro de uma raiz em sua AWS organização, você deve ter as seguintes permissões:

- `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations
- `organizations:UpdateOrganizationalUnit`

### AWS Management Console

Para renomear uma UO

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue até a UO que você quer renomear e execute uma das seguintes etapas:
   - Selecione o botão de opção
     
     ao lado da instância da UO que deseja renomear. Em seguida, no menu Actions (Ações), em Organizational unit (Unidade organizacional), escolha Rename (Renomear).
   - Escolha o nome da UO para acessar a página de detalhes da UO. Depois, na parte superior da página, escolha Rename (Renomear).
3. Na caixa de diálogo Rename organizational unit (Renomear unidade organizacional), insira um novo nome e escolha Save changes (Salvar alterações).

### AWS CLI & AWS SDKs

Para renomear uma UO

Você pode usar um dos seguintes comandos para renomear uma UO:

- AWS CLI: update-organizational-unit

  O exemplo a seguir mostra como renomear uma UO.

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
```

```
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- AWS SDKs: UpdateOrganizationalUnit

## Edição de tags anexadas a uma UO

Quando faz login na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a uma UO. Para fazer isso, conclua as seguintes etapas.

> **Permissões mínimas**
>
> Para editar as tags anexadas a uma OU dentro de uma raiz em sua AWS organização, você deve ter as seguintes permissões:
>
> - `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations
> - `organizations:DescribeOrganizationalUnit` – necessária somente ao usar o console do Organizations
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

Para editar de tags anexadas a uma UO

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, navegue e escolha o nome da UO cujas tags você quer editar.
3. Na página de detalhes da UO, escolha a guia Tags, depois escolha Manage tags (Gerenciar tags).

4. Você pode executar qualquer uma das seguintes ações nesta guia:

   - Edite o valor de qualquer tag inserindo um novo valor sobre o antigo. Não é possível modificar a chave de tag. Para alterar uma chave, é preciso excluir a tag com a chave antiga e adicionar uma tag com a nova chave.
   - Remova uma tag existente escolhendo Remove (Remover) ao lado da tag que você deseja remover.
   - Adicione um novo par de chave e valor de tag. Escolha Add tag (Adicionar tag) e insira o novo nome da chave e o valor opcional nas caixas fornecidas. Se você deixar a caixa Value (Valor) vazia, o valor é uma sequência vazia, não é `null`.

5. Escolha Save changes (Salvar alterações) depois de ter feito todas as adições, remoções e edições que deseja fazer.

AWS CLI & AWS SDKs

Para editar de tags anexadas a uma UO

Você pode usar um dos seguintes comandos para alterar as tags anexadas a uma UO:

- AWS CLI: tag-resource e untag-resource

  O exemplo a seguir anexa tag `"Department"="12345"` a uma UO. Observe que `Key` e `Value` diferenciam entre maiúsculas e minúsculas.

  ```
  $ aws organizations tag-resource \
      --resource-id ou-a1b2-f6g7h222 \
      --tags Key=Department,Value=12345
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

  O exemplo a seguir remove a tag `Department` de uma UO.

  ```
  $ aws organizations untag-resource \
      --resource-id ou-a1b2-f6g7h222 \
      --tag-keys Department
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS SDKs: TagResourcee UntagResource

# Movimentação de contas para uma UO ou entre a raiz e as UOs

Quando faz login na conta de gerenciamento de sua organização, você pode mover as contas de sua organização da raiz para uma UO, de uma UO para outra ou de uma UO de volta para a raiz. Colocar uma conta dentro de uma UO a submete às políticas que estão anexadas à UO superior e às outras UOs na cadeia da superior até a raiz. Se a conta não estiver em uma UO, estará sujeita apenas às políticas que estão anexadas diretamente à raiz e a todas que estiverem anexadas diretamente à conta. Para mover contas, conclua as seguintes etapas.

Permissões mínimas

Para mover contas para um novo local na hierarquia da UO, você precisa ter as seguintes permissões:

- `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations
- `organizations:MoveAccount`

AWS Management Console

Para mover contas para uma UO

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, encontre a conta ou as contas que você deseja mover. Você pode navegar na hierarquia da UO ou habilitar View Contas da AWS only (Exibir apenas Contas da AWS ) para ver uma lista simples de contas sem a estrutura da UO. Se você tiver muitas contas, talvez seja necessário escolher Load more accounts in 'ou-name' (Carregar mais contas em ‘nome-uo’) no fim da lista para encontrar todas que você deseja mover.
3. Escolha a caixa de seleção
   ☑
   ao lado do nome de cada conta na que você deseja mover.
4. No menu Ações (Actions), em Conta da AWS, escolha Move (Mover).
5. Na caixa de diálogo Move Conta da AWS(Mover Conta da AWS), escolha a UO ou a raiz para a qual você quer mover a conta e escolha Move Conta da AWS(Mover Conta da AWS).

AWS CLI & AWS SDKs

Para mover uma conta para uma UO

Você pode usar um dos seguintes comandos para mover uma conta:

- AWS CLI: move-account

  O exemplo a seguir move an Conta da AWS da raiz para uma OU. Observe que é preciso especificar os IDs dos contêineres de origem e de destino.

  ```
  $ aws organizations move-account \
      --account-id 111122223333 \
      --source-parent-id r-a1b2 \
      --destination-parent-id ou-a1b2-f6g7h111
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS SDKs: MoveAccount

# Excluir UOs

Quando faz login na conta de gerenciamento de sua organização, você pode excluir UOs que não sejam mais necessárias.

Primeiro é preciso mover todas as contas para fora da UO e das UOs subordinadas, para depois poder excluir as UOs subordinadas.

> **Permissões mínimas**
>
> Para excluir uma UO, você precisa ter as seguintes permissões:
>
> - `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations
> - `organizations:DeleteOrganizationalUnit`

### AWS Management Console

#### Para excluir uma UO

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Contas da AWS, encontre as UOs que você deseja excluir e escolha a caixa de seleção

   ao lado do nome de cada UO.
3. Selecione Actions (Ações) e, em Organizational unit (Unidade organizacional), escolha Delete (Excluir).
4. Para confirmar que deseja excluir as UOs, insira o nome da UO (se você optou por excluir apenas uma) ou a palavra 'delete (excluir)' (se você escolheu mais de uma) e, em seguida, escolha Delete (Excluir).

   AWS Organizations exclui as OUs e as remove da lista.

### AWS CLI & AWS SDKs

#### Como excluir uma UO

Você pode usar um dos seguintes comandos para excluir uma UO:

- AWS CLI: delete-organizational-unit

  O exemplo a seguir mostra como excluir uma UO.

  ```
  $ aws organizations delete-organizational-unit \
      --organizational-unit-id ou-a1b2-f6g7h222
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS SDKs: DeleteOrganizationalUnit

# Marcando atributos AWS Organizations

Uma tag é um rótulo de atributo personalizado que você adiciona a um recurso da AWS para facilitar a identificação, organização e pesquisa de recursos. Cada tag tem duas partes:

- Uma chave de tag (por exemplo `CostCenter`, `Environment` ou `Project`). As chaves de tag podem ter até 128 caracteres e diferenciam minúsculas de maiúsculas.
- Um valor de tag (por exemplo, `111122223333` ou `Production`). Os valores de tag podem ter até 256 caracteres e, como as chaves de tag, diferenciam minúsculas de maiúsculas. É possível definir o valor de uma tag em uma string vazia, mas não configurar o valor de um tag como nula. Omitir o valor da tag é o mesmo que usar uma string vazia.

Para obter mais informações sobre quais são os caracteres permitidos em uma chave ou valor de tag, consulte Parâmetro Tags da API de tag na Referência da API de marcação dos Resource Groups.

Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. Para obter mais informações, consulte Melhores práticas para marcar AWS recursos.

> **Tip**
>
> Use políticas de tag para ajudar a padronizar as tags entre os recursos nas contas de sua organização.

Atualmente, o AWS Organizations suporta as seguintes operações de marcação quando você fez login na conta de gerenciamento:

- Você pode adicionar tags aos seguintes tipos de recurso da organização:
  - Contas da AWS
  - Unidades organizacionais
  - A raiz da organização
  - Políticas

Você pode adicionar tags nos seguintes momentos:

- Ao criar o recurso — Especifique as tags no console do Organizations ou use o parâmetro `Tags` com uma das operações de API `Create`. Isso não é aplicável à raiz da organização.
- Depois de criar o recurso — Use o console do Organizations ou chame a operação `TagResource`.

Você pode visualizar as tags em qualquer um dos recursos marcáveis no AWS Organizations usando o console ou chamando a operação `ListTagsForResource`.

É possível remover tags de um recurso especificando as chaves a remover usando o console ou chamando a operação `UntagResource`.

# Usar tags

As tags ajudam você a organizar recursos em sua organização, permitindo que você os agrupe por quaisquer categorias que sejam úteis para você. Por exemplo, você pode atribuir uma tag "Departmento" que rastreia o departamento responsável. Você pode atribuir uma tag "Ambiente" para rastrear se um determinado recurso faz parte de seus ambientes alfa, beta, gama ou produção.

Você também pode usar tags para:

- Aplique padrões de marcação em seus recursos.
- Controle quem pode acessar seus recursos

# Adição, atualização e remoção de tags

Quando faz login na conta de gerenciamento da sua organização, você pode adicionar tags aos recursos da sua organização.

## Adição de tags a um recurso ao criá-lo

Permissões mínimas

Para adicionar tags a um recurso ao criá-lo, você precisa das seguintes permissões:

- Permissão para criar um recurso do tipo especificado
- `organizations:TagResource`
- `organizations:ListTagsForResource` – necessário somente ao usar o console do Organizations

Você pode incluir chaves e valores de tag que são anexados aos seguintes recursos à medida que os cria.

- Conta da AWS
  - Conta criada
  - Conta convidada
- Unidade organizacional (UO)
- Política
  - Política de cancelamento de serviços de IA
  - Política de backup
  - Política de controle de serviço
  - Política de tag

A raiz da organização é criada quando você cria inicialmente a organização, portanto, você só pode adicionar tags a ela como um recurso existente.

## Adição ou atualização de tags para um aplicativo existente

Você também pode adicionar novas tags ou atualizar os valores das tags anexadas aos recursos existentes.

> **Permissões mínimas**
>
> Para adicionar ou atualizar tags de recursos na sua organização, você precisa das seguintes permissões:
>
> - `organizations:TagResource`
> - `organizations:ListTagsForResource` – necessário somente ao usar o console do Organizations
>
> Para remover tags de recursos na sua organização, você precisa das seguintes permissões:
>
> - `organizations:UntagResource`

AWS Management Console

Para adicionar, atualizar ou remover tags de um recurso existente

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Navegue e escolha a conta, a raiz, a UO ou a política e clique em seu nome para abrir sua página de detalhes.
3. Na guia Tags (Tags), selecione Manage tags (Gerenciar tags).
4. É possível adicionar novas tags, modificar os valores das tags existentes ou remover tags.

   Para adicionar uma tag, escolha Add Tag (Adicionar tag) e insira uma chave e um valor para cada tag.

   Para remover uma tag, selecione Remover.

   As chaves e valores das tags diferenciam maiúsculas de minúsculas. Use a capitalização na qual você deseja padronizar. Você também deve atender aos requisitos de quaisquer políticas de tag aplicáveis.
5. Repita a etapa anterior quantas vezes precisar.
6. Escolha Salvar alterações.

AWS CLI & AWS SDKs

Adicionar ou atualizar as tags de um recurso existente

Você pode usar um dos seguintes comandos para adicionar tags aos recursos marcáveis na sua organização:

- AWS CLI: tag-resource
- AWSSDKs: TagResource

Para excluir tags de um recurso na sua organização

Você pode usar um dos seguintes comandos para excluir tags:

- AWS CLI: untag-resource

- AWSSDKs: UntagResource

# Usar o AWS Organizations com outros serviços da AWS

Você pode usar o acesso confiável para habilitar um serviço compatível da AWS que você especificar, chamado serviço confiável, a executar tarefas em sua organização e suas contas em seu nome. Isso requer a concessão de permissões ao serviço confiável, mas não afeta as permissões para usuários ou perfis. Quando você habilita o acesso, o serviço confiável pode criar uma função do IAM denominada função vinculada ao serviço em todas as contas de sua organização sempre que a função for necessária. Essa função tem uma política de permissões que consente que o serviço confiável realize as tarefas que estão descritas na documentação do serviço. Isso permite que você especifique configurações e detalhes de configuração que deseja que o serviço confiável mantenha nas contas de sua organização em seu nome. O serviço confiável só cria funções vinculadas ao serviço quando precisa executar ações de gerenciamento em contas, e não necessariamente em todas as contas da organização.

**Important**

Recomendamos enfaticamente que, quando a opção estiver disponível, habilitar e desabilitar o acesso confiável usando somente o console do serviço confiável ou suas equivalentes de operação da AWS CLI ou API. Isso permite que o serviço confiável execute qualquer inicialização necessária ao habilitar o acesso confiável, como a criação de recursos necessários e a limpeza necessária de recursos ao desabilitar o acesso confiável.
Para obter informações sobre como habilitar ou desabilitar o acesso a serviços confiáveis para sua organização usando o serviço confiável, consulte o link Saiba mais abaixo da coluna Supports Trusted Access (Suporta ao acesso confiável) em AWS serviços que você pode usar com AWS Organizations.
Se você desabilitar o acesso usando o console do Organizations, comandos de CLI ou operações de API, isso fará com que as seguintes ações ocorram:

- O serviço não pode mais criar uma função vinculada ao serviço nas contas de sua organização. Isso significa que o serviço não pode executar operações em seu nome em nenhuma conta nova de sua organização. O serviço ainda pode executar operações em contas mais antigas até que o serviço conclua sua limpeza a partir do AWS Organizations.
- O serviço não pode mais executar tarefas nas contas-membro da organização, a menos que essas operações sejam explicitamente permitidas pelas políticas do IAM anexadas às suas funções. Isto inclui qualquer agregação de dados das contas-membro para a conta de gerenciamento ou para uma conta de administrador delegado, quando relevante.

- Alguns serviços detectam isso e limpam quaisquer dados ou recursos remanescentes relacionados à integração, enquanto outros serviços param de acessar a organização, mas deixam quaisquer dados históricos e configurações implementadas, para suportar uma possível reativação da integração.

Em vez disso, usar o console ou comandos do outro serviço para desabilitar a integração garante que o outro serviço possa limpar todos os recursos necessários somente para a integração. A forma como o serviço limpa seus recursos nas contas da organização depende desse serviço. Para obter mais informações, consulte a documentação do serviço da AWS.

## Permissões necessárias para habilitar o acesso confiável

O acesso confiável exige permissões para dois serviços: o AWS Organizations e o serviço confiável. Para permitir o acesso confiável, escolha um dos seguintes cenários:

- Se você tiver credenciais com permissões no AWS Organizations e no serviço confiável, habilite o acesso usando as ferramentas (o console ou a AWS CLI) disponíveis no serviço confiável. Isso permite que o serviço confiável habilite o acesso confiável no AWS Organizations em seu nome e cria todos os recursos necessários para que o serviço opere em sua organização.

  As permissões mínimas para essas credenciais são as seguintes:

  - `organizations:EnableAWSServiceAccess`. Você pode usar também a chave de condição `organizations:ServicePrincipal` com essa operação para restringir as solicitações que essas operações fazem a uma lista de nomes de entidades primárias de serviço aprovadas. Para obter mais informações, consulte Chaves de condição.
  - `organizations:ListAWSServiceAccessForOrganization` – Necessário se você usa o console do AWS Organizations.
  - As permissões mínimas necessárias pelo serviço confiável dependem do serviço. Para obter mais informações, consulte a documentação do serviço confiável.
- Se uma pessoa tiver credenciais com permissões no AWS Organizations, mas outra pessoa tiver credenciais com permissões no serviço confiável, realize estas etapas na seguinte ordem:
  1. A pessoa que tem credenciais com permissões no AWS Organizations deve usar o console do AWS Organizations, a AWS CLI ou um SDK da AWS para permitir o acesso confiável para o serviço confiável. Isso concede permissão para que outros serviços executem sua configuração necessária na organização quando a etapa seguinte (etapa 2) é realizada.

As permissões mínimas do AWS Organizations são as seguintes:

- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization` – Necessário somente se você usa o console do AWS Organizations

Sobre as etapas específicas para permitir acesso confiável no AWS Organizations, consulte Como habilitar ou desabilitar o acesso confiável.

2. A pessoa que tem credenciais com permissões no serviço confiável permite que esse serviço funcione com o AWS Organizations. Isso instrui o serviço a realizar qualquer inicialização necessária, como a criação de recursos necessários para que o serviço confiável opere na organização. Para obter mais informações, consulte as instruções específicas do serviço em AWS serviços que você pode usar com AWS Organizations.

## Permissões necessárias para desabilitar o acesso confiável

Quando você não quiser mais permitir que o serviço confiável opere em sua organização ou suas contas, escolha um dos seguintes cenários.

> **Important**
>
> Desabilitar o acesso ao serviço confiável não impede que os usuários e as funções com permissões apropriadas usem esse serviço. Para impedir completamente que usuários e perfis acessem um serviço da AWS, você pode remover as permissões do IAM que concedem o acesso ou usar políticas de controle de serviço (SCPs) no AWS Organizations. Você pode aplicar SCPs somente às contas-membro. As SCPs não se aplicam à conta de gerenciamento. Recomendamos que você não execute serviços na conta de gerenciamento. Em vez disso, execute-os em contas-membro, onde você pode controlar a segurança usando SCPs.

- Se você tiver credenciais com permissões no AWS Organizations e no serviço confiável, desabilite o acesso usando as ferramentas (o console ou a AWS CLI) disponíveis para o serviço confiável. Em seguida, o serviço faz a limpeza, removendo recursos que não são mais necessários e desabilitando o acesso confiável do serviço no AWS Organizations em seu nome.

  As permissões mínimas para essas credenciais são as seguintes:

- `organizations:DisableAWSServiceAccess`. Você pode usar também a chave de condição `organizations:ServicePrincipal` com essa operação para restringir as solicitações que essas operações fazem a uma lista de nomes de entidades primárias de serviço aprovadas. Para obter mais informações, consulte Chaves de condição.
- `organizations:ListAWSServiceAccessForOrganization` – Necessário se você usa o console do AWS Organizations.
- As permissões mínimas necessárias pelo serviço confiável dependem do serviço. Para obter mais informações, consulte a documentação do serviço confiável.

- Se as credenciais com permissões no AWS Organizations não forem as credenciais com permissões no serviço confiável, realize estas etapas na seguinte ordem:
  1. A pessoa com permissões no serviço confiável primeiro desabilita o acesso usando esse serviço. Isso instrui o serviço confiável a fazer a limpeza removendo os recursos necessários para o acesso confiável. Para obter mais informações, consulte as instruções específicas do serviço em AWS serviços que você pode usar com AWS Organizations.
  2. A pessoa com permissões no AWS Organizations pode usar o console do AWS Organizations, a AWS CLI ou um SDK da AWS para desabilitar o acesso para o serviço confiável. Isso remove as permissões para o serviço confiável de sua organização e de suas contas.

     As permissões mínimas do AWS Organizations são as seguintes:

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – Necessário somente se você usa o console do AWS Organizations

     Sobre as etapas específicas para não permitir acesso confiável no AWS Organizations, consulte Como habilitar ou desabilitar o acesso confiável.

## Como habilitar ou desabilitar o acesso confiável

Se você tiver permissões somente para o AWS Organizations e quiser habilitar ou desabilitar o acesso confiável para sua organização em nome do administrador de outro serviço da AWS, use o procedimento a seguir.

> **Important**
>
> Recomendamos enfaticamente que, quando a opção estiver disponível, habilitar e desabilitar o acesso confiável usando somente o console do serviço confiável ou suas equivalentes

de operação da AWS CLI ou API. Isso permite que o serviço confiável execute qualquer inicialização necessária ao habilitar o acesso confiável, como a criação de recursos necessários e a limpeza necessária de recursos ao desabilitar o acesso confiável.
Para obter informações sobre como habilitar ou desabilitar o acesso a serviços confiáveis para sua organização usando o serviço confiável, consulte o link Saiba mais abaixo da coluna Supports Trusted Access (Suporta ao acesso confiável) em AWS serviços que você pode usar com AWS Organizations.
Se você desabilitar o acesso usando o console do Organizations, comandos de CLI ou operações de API, isso fará com que as seguintes ações ocorram:

- O serviço não pode mais criar uma função vinculada ao serviço nas contas de sua organização. Isso significa que o serviço não pode executar operações em seu nome em nenhuma conta nova de sua organização. O serviço ainda pode executar operações em contas mais antigas até que o serviço conclua sua limpeza a partir do AWS Organizations.
- O serviço não pode mais executar tarefas nas contas-membro da organização, a menos que essas operações sejam explicitamente permitidas pelas políticas do IAM anexadas às suas funções. Isto inclui qualquer agregação de dados das contas-membro para a conta de gerenciamento ou para uma conta de administrador delegado, quando relevante.
- Alguns serviços detectam isso e limpam quaisquer dados ou recursos remanescentes relacionados à integração, enquanto outros serviços param de acessar a organização, mas deixam quaisquer dados históricos e configurações implementadas, para suportar uma possível reativação da integração.

Em vez disso, usar o console ou comandos do outro serviço para desabilitar a integração garante que o outro serviço possa limpar todos os recursos necessários somente para a integração. A forma como o serviço limpa seus recursos nas contas da organização depende desse serviço. Para obter mais informações, consulte a documentação do serviço da AWS.

AWS Management Console

Habilitar o acesso de serviço confiável

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

2. Na página Services (Serviços), localize a linha do serviço que você deseja habilitar e escolha seu nome.
3. Escolha Enable trusted access (Habilitar acesso confiável).
4. Na caixa de diálogo de confirmação, marque a caixa para Show the option to enable trusted access (Mostrar a opção para habilitar o acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Ativar o acesso confiável).
5. Se você estiver habilitando acesso, informe ao administrador do outro serviço da AWS que ele agora pode habilitar o outro serviço para funcionar com o AWS Organizations.

Para desabilitar acesso a serviço confiável

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do serviço que você deseja desabilitar e escolha seu nome.
3. Aguarde até que o administrador do outro serviço informe que o serviço está desabilitado e que os recursos foram limpos.
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Desabilitar acesso confiável.

AWS CLI, AWS API

Para habilitar ou desabilitar acesso a serviço confiável

Você pode usar os comandos da AWS CLI ou as operações de API a seguir para habilitar ou desabilitar o acesso ao serviço confiável:

- AWS CLI: AWS organizations enable-aws-service-access
- AWS CLI: AWS organizations disable-aws-service-access
- AWS API: EnableAWSServiceAccess
- AWS API: DisableAWSServiceAccess

# AWS Organizations e funções vinculadas ao serviço

O AWS Organizations usa funções vinculadas ao serviço do IAM para permitir que os serviços confiáveis realizem tarefas em seu nome nas contas-membro da organização. Quando você configura um serviço confiável e o autoriza a se integrar com sua organização, esse serviço pode solicitar que o AWS Organizations crie uma função vinculada ao serviço em sua conta-membro. O serviço confiável faz isso de forma assíncrona, conforme a necessidade, e não obrigatoriamente em todas as contas da organização ao mesmo tempo. A função vinculada ao serviço tem permissões predefinidas do IAM que possibilitam que outro serviço confiável realize tarefas específicas nessa conta. Em geral, a AWS gerencia todas as funções vinculadas ao serviço, o que significa que você geralmente não pode alterar as funções ou as políticas anexadas.

Para tornar tudo isso possível, quando você criar uma conta em uma organização ou aceitar um convite para ingressar sua conta existente em uma organização, o AWS Organizations faz a provisão da conta-membro com uma função vinculada ao serviço denominada `AWSServiceRoleForOrganizations`. Somente o próprio serviço do AWS Organizations pode assumir essa função. A função tem permissões que possibilitam que o AWS Organizations crie funções vinculadas ao serviço para outros serviços da AWS. Essa função vinculada ao serviço está presente em todas as organizações.

Embora não seja recomendável, se sua organização tiver apenas os recursos de faturamento consolidado habilitados, a função vinculada a serviço denominada `AWSServiceRoleForOrganizations` nunca será usada e você poderá excluí-la. Para habilitar posteriormente todos os recursos em sua organização, a função será necessária e deverá ser restaurada. As seguintes verificações ocorrem quando você inicia o processo para ativar todos os recursos:

- Para cada conta-membro que foi convidada a ingressar na organização – O administrador da conta recebe uma solicitação para concordar em habilitar todos os recursos. Para aceitar a solicitação corretamente, o administrador deve ter as permissões `organizations:AcceptHandshake` e `iam:CreateServiceLinkedRole` caso a função vinculada ao serviço (`AWSServiceRoleForOrganizations`) ainda não exista. Se a função `AWSServiceRoleForOrganizations` já existir, o administrador precisa apenas da permissão `organizations:AcceptHandshake` para concordar com a solicitação. Quando o administrador concordar com a solicitação, o AWS Organizations criará a função vinculada ao serviço, caso ela não exista.

- Para cada conta-membro que foi criada na organização – O administrador da conta recebe uma solicitação para recriar a função vinculada ao serviço. (O administrador da conta-membro não recebe uma solicitação para habilitar todos os recursos, pois o administrador da conta de gerenciamento (antes conhecida como "conta mestra") é considerado o proprietário das contas-membro criadas.) O AWS Organizations cria a função vinculada ao serviço quando o administrador da conta-membro aceita com a solicitação. O administrador deve ter as permissões `organizations:AcceptHandshake` e `iam:CreateServiceLinkedRole` para aceitar com êxito o handshake.

Após ativar todos os recursos em sua organização, você não poderá mais excluir a função vinculada ao serviço `AWSServiceRoleForOrganizations` de qualquer conta.

> **Important**
>
> As SCPs do AWS Organizations nunca afetam as funções vinculadas a serviço. Essas funções são isentas de quaisquer restrições da SCP.

## AWS serviços que você pode usar com AWS Organizations

Com AWS Organizations você pode realizar atividades de gerenciamento de contas em grande escala, consolidando várias Contas da AWS em uma única organização. A consolidação de contas simplifica a forma como você usa outros AWS serviços. Você pode aproveitar os serviços de gerenciamento de várias contas disponíveis em AWS Organizations alguns AWS serviços para realizar tarefas em todas as contas que são membros da sua organização.

A tabela a seguir lista AWS os serviços que você pode usar com AWS Organizations e os benefícios de usar cada serviço em nível organizacional.

Acesso confiável — Você pode habilitar um AWS serviço compatível para realizar operações Contas da AWS em toda a sua organização. Para ter mais informações, consulte Usar o AWS Organizations com outros serviços da AWS.

Administrador delegado para AWS serviços — Um AWS serviço compatível pode registrar uma conta de AWS membro na organização como administrador das contas da organização nesse serviço. Para ter mais informações, consulte Administrador delegado para serviços da AWS que funcionam com o Organizations.

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Account Management<br><br>Gerencie os detalhes e os metadados de todos Contas da AWS os da sua organização. | Você pode criar, atualizar e excluir as informações de contato alternativas de todas as contas da sua organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |
| AWS Application Migration Service<br><br>AWS Application Migration Service permite que as empresas lift-and-shift acessem AWS um grande número de servidores | Você pode gerenciar migrações em grande escala em várias contas. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| físicos, virtuais ou em nuvem sem problemas de compatibilidade, interrupção no desempenho ou longos períodos de transição. | | | | |
| AWS Artifact<br><br>Baixe relatórios AWS de conformidade de segurança, como relatórios ISO e PCI. | É possível aceitar contratos em nome de todas as contas da sua organização. |  Sim<br><br>Saiba mais |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Audit Manager<br><br>Automatize a coleta contínua de evidências para ajudá-lo a auditar seu uso de serviços de nuvem. | Audite continuamente seu AWS uso em várias contas em sua organização para simplificar a forma como você avalia o risco e a conformidade. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Backup<br><br>Gerencie e monitore backups em todas as contas da sua organização. | Você pode configurar e gerenciar planos de backup para toda a organização ou para grupos de contas nas unidades organizacionais (UOs). Você pode monitorar centralmente backups de todas as suas contas. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado |
|---|---|---|---|
| AWS Billing and Cost Management<br><br>Fornece uma visão geral dos dados de gerenciamento financeiro AWS na nuvem e ajuda você a tomar decisões mais rápidas e informadas. | Permite que os dados de alocação de custos divididos recuperem AWS Organizations informações, se aplicável, e coletem dados de telemetria para os serviços de dados de alocação de custos divididos pelos quais você optou.<br><br>Para obter mais |  Sim<br><br>Saiba mais |  Não |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | informações, consulte O que é AWS Billing and Cost Management? no guia do usuário do Billing and Cost Management. | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| StackSets do AWS CloudFormation<br><br>Crie, atualize ou exclua pilhas em várias contas e regiões com uma única operação. | Um usuário na conta de gerenciamento ou em uma conta de administrador delegado pode criar um conjunto de pilhas com permissões gerenciadas por serviço que implante instâncias de pilha nas contas de sua organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS CloudTrail<br><br>Habilite governança, conformidade e auditorias operacionais e de risco da conta. | Um usuário em uma conta de gerenciamento ou conta de administrador delegado pode criar uma trilha de organização ou armazenamento de dados de eventos que registre em log todos os eventos de todas as contas na organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado |
|---|---|---|---|
| AWS Compute Optimizer<br><br>Obtenha recomendações de otimização AWS computacional. | Você poderá analisar todos os recursos que estiverem nas contas da sua organização para obter recomendações de otimização.<br><br>Para obter mais informações, consulte Contas suportadas pelo Compute Optimizer no Guia do |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | usuário do AWS Compute Optimizer. | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Config<br><br>Avalie e audite as configurações dos recursos da AWS . | É possível obter uma visualização do status de conformidade de toda a organização. Você também pode usar operações de AWS Config API para gerenciar AWS Config regras e pacotes de conformidade Contas da AWS em toda a sua |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais:<br><br>Config Rules<br><br>Pacotes de conformidade<br><br>Agregação de dados de várias regiões e várias contas | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | organização.<br><br>Você pode usar uma conta de administrador delegado para agregar dados de configuração e compatibilidade de recursos de todas as contas-membro de uma organização no AWS Organizations. Para obter mais informaçõ | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | es, consulte Registrar um administrador delegado no Guia do desenvolvedor do AWS Config . | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Control Tower<br><br>Configure e controle um ambiente multiconta da AWS seguro e compatível. | Você pode configurar uma landing zone, um ambiente com várias contas para todos os seus AWS recursos. Esse ambiente inclui uma organização e entidades da organização. Você pode usar esse ambiente para impor normas |  Sim<br><br>Saiba mais |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | de conformidade em todos os seus Contas da AWS.<br><br>Para obter mais informações, consulte Como o AWS Control Tower e Gerenciar contas por meio do AWS Organizations no Guia do usuário do AWS Control Tower . | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado |
|---|---|---|---|
| Hub de Otimização de Custos da AWS<br><br>Reúna recomendações de custo em todos os produtos de AWS otimização. | Você pode identificar, filtrar e agregar facilmente recomendações de otimização de AWS custos em suas contas de AWS Organizations membros e AWS regiões.<br><br>Para obter mais informações, consulte Cust Optimization Hub no guia do |  Sim<br><br>Saiba mais |  Não |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | usuário do Cost Optimization Hub. | | | |
| Amazon Detective<br><br>Gere visualizações baseadas em seus dados de log para analisar, investigar e identificar rapidamente a causa raiz das descobertas de segurança ou atividades suspeitas. | Você pode integrar o Amazon Detective AWS Organizations para garantir que seu gráfico de comportamento de detetive forneça visibilidade da atividade de todas as contas da sua organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| DevOpsGuru da Amazon<br><br>Analise dados operacionais e métricas e eventos de aplicações para identificar comportamentos que se desviam dos padrões operacionais normais. Os usuários são notificados quando o DevOps Guru detecta um problema ou risco operacional. | Você pode se integrar AWS Organizations para gerenciar insights de todas as contas em toda a organização. Você delega um administrador para visualizar, classificar e filtrar insights de todas as contas para obter a integridade em toda a organização de |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | todas as aplicações monitoradas. | | | |
| AWS Directory Service<br><br>Configure e execute diretórios na AWS nuvem ou conecte seus AWS recursos a um Microsoft Active Directory local existente. | Você pode se integrar AWS Organizations para AWS Directory Service compartilhar diretórios sem interrupções entre várias contas e qualquer VPC em uma região. |  Sim<br><br>Saiba mais |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Amazon EventBridge<br><br>Monitore seus AWS recursos e os aplicativos que você executa AWS em tempo real. | Você pode ativar o compartilhamento de todos os EventBridge eventos da Amazon, anteriormente Amazon CloudWatch Events, em todas as contas da sua organização.<br><br>Para obter mais informações, consulte Enviar e receber |  Não |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | EventBridge eventos da Amazon Contas da AWS no Guia do EventBridge usuário da Amazon. | | | |
| AWS Firewall Manager<br><br>Configurar e gerenciar centralmente regras de firewall de aplicativos web entre contas e aplicativos. | Você pode configurar e gerenciar centralmente AWS WAF as regras em todas as contas da sua organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Amazon GuardDuty<br><br>GuardDuty é um serviço contínuo de monitoramento de segurança que analisa e processa informações de uma variedade de fontes de dados. Ele usa feeds de inteligência sobre ameaças e machine learning para identificar atividades inesperadas e potencialmente não autorizadas e maliciosas no seu ambiente da AWS . | Você pode designar uma conta de membro para visualizar e gerenciar GuardDuty todas as contas da sua organização. A adição de contas de membros ativa GuardDuty automaticamente essas contas na lista selecionada da Região da AWS. Você |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | também pode automatizar a GuardDuty ativação de novas contas adicionadas à sua organização.<br><br>Para obter mais informações, consulte GuardDuty Organizations in the Amazon GuardDuty User Guide. | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Health<br><br>Obtenha visibilidade dos eventos que podem afetar o desempenho dos recursos ou os problemas de disponibilidade AWS dos serviços. | Você pode agregar AWS Health eventos em todas as contas da sua organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Identity and Access Management<br><br>Controle com segurança o acesso aos AWS recursos. | Você pode usar os dados de serviços acessados mais recentemente no IAM para ajudá-lo a entender melhor a atividade da AWS em sua organização. Você pode usar esses dados para criar e atualizar políticas de controle de serviço (SCPs) que |  Não |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | restringem o acesso apenas aos serviços da AWS que as contas de sua organização usam.<br><br>Para obter um exemplo, consulte Uso de dados para refinar permissões para uma unidade organizacional no Guia do usuário do IAM. | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| IAM Access Analyzer<br><br>Analise as políticas baseadas em recursos em seu AWS ambiente para identificar quaisquer políticas que concedam acesso a um principal fora de sua zona de confiança. | Você pode designar uma conta-membro como administrador do IAM Access Analyzer.<br><br>Para obter mais informações, consulte Habilitar o Access Analyzer no Guia do usuário do IAM. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Amazon Inspector<br><br>Analise automaticamente suas AWS cargas de trabalho em busca de vulnerabilidades para descobrir instâncias do Amazon EC2 e imagens de contêineres que residem no Amazon ECR em busca de vulnerabilidades de software e exposição não intencional na rede. | Delegue um administrador para habilitar ou desabilitar verificações de contas-membro, exibir dados de localização agregados de toda a organização, criar e gerenciar regras de supressão.<br><br>Para obter mais informações, consulte Gerenciar |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | várias contas com o AWS Organizations no Guia do usuário do Amazon Inspector. | | | |
| AWS License Manager<br><br>Simplifique o processo de levar licenças de software de fornecedor para a nuvem. | É possível habilitar a descoberta entre contas de recursos de computação em toda a sua organização. |  Sim<br><br>Saiba mais |  <br><br>Saiba mais | Sim |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Amazon Macie<br><br>Detecta e classifica conteúdo essencial para os negócios usando machine learning para ajudar você a atender aos requisitos de segurança e privacidade de dados. Ele avalia continuamente o conteúdo armazenado no Amazon S3 e notifica você sobre possíveis problemas. | É possível configurar o Amazon Macie para todas as contas de sua organização para ter uma visão consolidada de todos os dados no Amazon S3, em todas as contas, a partir de uma conta de administrador designado do Macie. Você pode |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | configurar o Macie para proteger automaticamente os recursos em novas contas à medida que sua organização cresce. Você é alertado para corrigir configurações incorretas de políticas nos buckets do S3 em toda a sua | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado |
|---|---|---|---|
| | organização. | | |
| AWS Marketplace<br><br>Um catálogo digital selecionado que você pode usar para encontrar, comprar, implantar e gerenciar o software, os dados e os serviços de terceiros de você que precisa para desenvolver soluções e administrar sua empresa. | Você pode compartilhar licenças para suas AWS Marketplace assinaturas e compras em todas as contas da sua organização. |  Sim<br><br>Saiba mais |  Não |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Marketplace<br>Marketplace privado<br><br>Fornece um amplo catálogo de produtos disponíveis em AWS Marketplace, juntamente com um controle refinado desses produtos. | Permite criar várias experiências de mercado privadas associadas a toda a sua organização, a uma ou mais OUs ou a uma ou mais contas em sua organização, cada uma com seu próprio conjunto de produtos aprovados. Seus AWS administr |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | adores também podem aplicar a marca da empresa a cada experiência de mercado privado com o logotipo, as mensagens e o esquema de cores da sua empresa ou equipe. | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Gerenciador de rede AWS<br><br>Permite que você gerencie centralmente sua rede principal de AWS Cloud WAN e sua rede AWS Transit Gateway em todas as AWS contas, regiões e locais locais. | Você pode gerenciar e monitorar centralmente suas redes globais com gateways de trânsito e seus recursos conectados em várias AWS contas em sua organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Amazon Q Developer<br><br>O Amazon Q Developer é um assistente de conversação com inteligência artificial generativa (IA) que pode ajudar você a entender, criar, ampliar e operar AWS aplicativos. | A versão de assinatura paga do Amazon Q Developer requer integração com Organizations. |  Sim<br><br>Saiba mais |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Resource Access Manager<br><br>Compartilhe AWS recursos específicos que você possui com outras contas. | É possível compartilhar recursos em sua organização sem trocar convites adicionais. Os recursos que você pode compartilhar incluem regras do Route 53 Resolver, reservas de capacidade sob demanda e muito mais.<br><br>Para obter |  Sim<br><br>Saiba mais |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | informações sobre compartilhamento de reservas de capacidade, consulte o Guia do usuário do Amazon EC2 para instâncias do Linux ou o Guia do usuário do Amazon EC2 para instâncias do Windows.<br><br>Para obter uma lista de recursos | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | compartilháveis, consulte Recursos compartilháveis no Guia do usuário do AWS RAM . | | | |
| Explorador de recursos da AWS<br><br>Explore seus recursos por meio de uma experiência semelhante ao uso de um mecanismo de pesquisa na Internet. | Habilite a pesquisa em várias contas. |  Sim<br><br>Saiba mais |  <br><br>Saiba mais | Sim |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado |
|---|---|---|---|
| AWS Security Hub<br><br>Visualize seu estado de segurança AWS e verifique seu ambiente de acordo com os padrões e as melhores práticas de segurança do setor. | Você pode ativar automaticamente o Security Hub para todas as contas de sua organização, incluindo as novas contas à medida que forem adicionadas. Isso aumenta a cobertura para verificações e descobertas do Security Hub, o que |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | fornece uma imagem mais precisa do seu procedimento de segurança em geral. | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Amazon S3 Storage Lens<br><br>Tenha visibilidade das métricas de uso e atividade de armazenamento do Amazon S3 com recomendações acionáveis para otimizar o armazenamento. | Configure o Amazon S3 Storage Lens para ter visibilidade do uso de armazenamento e das tendências de atividade do Amazon S3, além de recomendações para todas as contas-membro de sua organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Amazon Security Lake<br><br>O Amazon Security Lake centraliza dados de segurança de fontes na nuvem, on-premises e personalizadas em um data lake armazenado em sua conta. | Crie um data lake que colete logs e eventos em suas contas. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Service Catalog<br><br>Crie e gerencie catálogos de serviços de TI aprovados para uso na AWS. | É possível compartilhar portfólios e copiar produtos entre contas com mais facilidade, sem compartilhar IDs de portfólio. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Service Quotas<br><br>Visualize e gerencie suas cotas de serviço, também conhecidas como limites, a partir de um local central. | É possível criar um modelo de solicitação de cota para solicitar automaticamente um aumento de cota quando contas na sua organização forem criadas. |  Sim<br><br>Saiba mais |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS IAM Identity Center<br><br>Forneça acesso de logon único para todas as contas e aplicativos de nuvem. | Os usuários podem entrar no portal de AWS acesso com suas credenciais corporativas e acessar recursos na conta de gerenciamento atribuída ou nas contas de membros. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado |
|---|---|---|---|
| AWS Systems Manager<br><br>Permita a visibilidade e o controle de seus AWS recursos. | Você pode sincronizar dados de operações Contas da AWS em toda a sua organização usando o Systems Manager Explorer.<br><br>Você pode gerenciar modelos, aprovações e relatórios de alteração para todas as contas-membro de sua |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| | organização a partir de uma conta de administrador delegado usando o Change Manager do Systems Manager. | | | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Políticas de tag<br><br>Use tags padronizadas entre todos os recursos das contas de sua organização. | Você pode criar políticas de tag para definir regras de atribuição de tags para recursos e tipos de recursos específicos, e anexar essas políticas às unidades e contas da organização para impor essas regras. |  Sim<br><br>Saiba mais |  Não | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| AWS Trusted Advisor<br><br>Trusted Advisor inspeciona seu AWS ambiente e faz recomendações quando existem oportunidades para economizar dinheiro, melhorar a disponibilidade e o desempenho do sistema ou ajudar a fechar lacunas de segurança. | Execute Trusted Advisor verificações para todos Contas da AWS em sua organização. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado |
|---|---|---|---|
| AWS Well-Architected Tool<br><br>AWS Well-Architected Tool Isso ajuda você a documentar o estado de suas cargas de trabalho e as compara com as melhores práticas AWS arquitetônicas mais recentes. | Permite que AWS WA Tool tanto os clientes quanto os clientes da Organizations simplifiquem o processo de compartilhamento de AWS WA Tool recursos com outros membros da organização. |  Sim<br><br>Saiba mais |  Não |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| IP Address Manager (IPAM) da Amazon VPC<br><br>O IPAM é um recurso de VPC que facilita o planejamento, o rastreamento e o monitoramento de endereços IP para AWS suas cargas de trabalho. | Monitore o uso de endereços IP em toda a organização e compartilhe grupos de endereços IP entre contas-membro. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

| AWS serviço | Benefícios de usar com AWS Organizations | Suporte a acesso confiável | Suporte a administrador delegado | |
|---|---|---|---|---|
| Amazon VPC Reachability Analyzer<br><br>O Reachability Analyzer é uma ferramenta de análise de configuração que possibilita a realização de testes de conectividade entre um recurso de origem e um recurso de destino em suas nuvens privadas virtuais (VPCs). | Monitore caminhos entre contas em suas organizações. |  Sim<br><br>Saiba mais |  Sim<br><br>Saiba mais | |

## AWS Account Management e AWS Organizations

O AWS Account Management ajuda você a gerenciar as informações e os metadados de todas as Contas da AWS da sua organização. Você pode definir, modificar ou excluir as informações de contato alternativas de cada uma das contas-membro da sua organização. Para obter informações, consulte Uso do AWS Account Management na sua organização no Guia do usuário do AWS Account Management.

Use as informações a seguir para ajudá-lo a integrar o AWS Account Management ao AWS Organizations.

## Para habilitar o acesso confiável no gerenciamento de contas

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

O gerenciamento de contas requer acesso confiável ao AWS Organizations para que você possa designar uma conta-membro como administrador delegado desse serviço em sua organização.

Você pode habilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Account Management, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Account Management que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Account Management como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

## Para desabilitar o acesso confiável no gerenciamento de contas

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador na conta de gerenciamento do AWS Organizations pode desabilitar acesso confiável com o AWS Account Management.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS Account Management e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).

5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Account Management que agora ele pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Account Management como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

## Habilitar uma conta de administrador delegado para o gerenciamento de contas

Quando você designa uma conta-membro como administrador delegado da organização, os usuários e as funções da conta designada podem gerenciar os metadados da Conta da AWS de outras contas-membro na organização. Se você não habilitar uma conta de administrador delegado, essas tarefas só poderão ser executadas pela conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento de detalhes da sua conta.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como administrador delegado para o gerenciamento de contas da organização

Para obter mais instruções sobre como configurar a política de delegação, consulte Criar ou atualizar uma política de delegação baseada em recursos.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, poderá usar os seguintes comandos:

- AWS CLI:

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

- AWS SDK: chame a operação `RegisterDelegatedAdministrator` do Organizations e o número de ID da conta-membro e identifique a entidade principal do serviço de conta `account.amazonaws.com` como parâmetros.

## AWS Application Migration Service (Serviço de migração de aplicativos) e AWS Organizations

AWS Application Migration Service simplifica, agiliza e reduz o custo da migração de aplicativos para o. AWS Com a integração ao Organizations, você pode usar o recurso de visualização global para gerenciar migrações em grande escala em várias contas. Para obter mais informações, consulte Configurando seu AWS Organizations no guia do usuário do Application Migration Service.

Use as informações a seguir para ajudá-lo a se integrar AWS Application Migration Service com AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Application Migration Service execute operações suportadas nas contas de sua organização em sua organização.

Você pode excluir ou modificar essa função somente se desativar o acesso confiável entre o Application Migration Service e o Organizations, ou se remover a conta do membro da organização.

- `AWSServiceRoleForApplicationMigrationService`

## Principais de serviços usados pelo Application Migration Service

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Serviço de Migração de Aplicativos concedem acesso às seguintes entidades de serviço:

- `mgn.amazonaws.com`

## Habilitando acesso confiável com o Application Migration Service

Ao habilitar o acesso confiável com o Application Migration Service, você pode usar o recurso de visualização global, que permite gerenciar migrações em grande escala em várias contas. A visão global fornece visibilidade e a capacidade de realizar ações específicas em servidores de origem, aplicativos e ondas em diferentes AWS contas. Para obter mais informações, consulte Configurando suas AWS Organizations no guia AWS Application Migration Service do usuário.

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode ativar o acesso confiável usando o AWS Application Migration Service console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Application Migration Service console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Application Migration Service realizar qualquer configuração necessária, como criar os recursos necessários ao serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Application Migration Service. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o AWS Application Migration Service console ou as ferramentas, não precisará concluir essas etapas.

Você pode ativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando ou chamando uma operação de API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Application Migration Service, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Application Migration Service que agora ele pode habilitar esse serviço usando seu console para trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitá-lo AWS Application Migration Service como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Ativar AWSServiceAccess

## Desabilitando o acesso confiável com o Application Migration Service

Somente um administrador na conta de gerenciamento da Organizations pode desativar o acesso confiável com o Application Migration Service.

Você pode desativar o acesso confiável usando as AWS Organizations ferramentas AWS Application Migration Service ou.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Application Migration Service console ou as ferramentas para desativar a integração com o Organizations. Isso permite AWS Application Migration Service realizar qualquer limpeza necessária, como excluir recursos ou funções de acesso que não são mais necessários para o serviço.
> Continue com estas etapas apenas se você não puder desabilitar a integração usando as ferramentas fornecidas pelo AWS Application Migration Service.
> Se você desabilitar o acesso confiável usando o AWS Application Migration Service console ou as ferramentas, não precisará concluir essas etapas.

Você pode desativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando do Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS Application Migration Service e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).

5. Se você for administrador do Only AWS Organizations, informe ao administrador AWS Application Migration Service que agora ele pode desativar esse serviço usando o console ou as ferramentas para não trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável a serviços:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar AWS Application Migration Service como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Desativar AWSServiceAccess

## Habilitando uma conta de administrador delegado para o Application Migration Service

Quando você designa uma conta membro como administrador delegado para a organização, os usuários e funções dessa conta podem realizar ações administrativas para o Serviço de Migração de Aplicativos que, de outra forma, só poderiam ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Serviço de Migração de Aplicativos. Para obter mais informações, consulte Configurando seu AWS Organizations no guia do usuário do Application Migration Service.

> **Permissões mínimas**
>
> Somente um usuário ou função na conta de gerenciamento da Organizations pode configurar uma conta de membro como administrador delegado para o Application Migration Service na organização.

AWS CLI, AWS API

Se quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos SDKs, você pode usar AWS os seguintes comandos:

- AWS CLI:

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

- AWS SDK: chame a `RegisterDelegatedAdministrator` operação da Organizations e o número de identificação da conta do membro e identifique o serviço da conta `mgn.amazonaws.com` como parâmetros.

### Desabilitando um administrador delegado para o Application Migration Service

Somente um administrador na conta de gerenciamento do Organizations pode remover um administrador delegado do Application Migration Service. É possível remover a conta de administrador delegado usando a operação `DeregisterDelegatedAdministrator` da CLI ou SDK do Organizations.

## AWS Artifact e AWS Organizations

AWS Artifact é um serviço que permite baixar relatórios de conformidade AWS de segurança, como relatórios ISO e PCI. Usando AWS Artifact, um usuário na conta de gerenciamento da organização pode aceitar automaticamente contratos em nome de todas as contas membros de uma organização, mesmo quando novos relatórios e contas são adicionados. Os usuários de contas-membro podem visualizar e fazer download dos contratos. Para obter mais informações, consulte Gerenciando um contrato para várias contas no AWS Artifact no Guia do AWS Artifact usuário.

Use as informações a seguir para ajudá-lo a se integrar AWS Artifact com AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite AWS Artifact realizar operações suportadas nas contas da sua organização em sua organização.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o AWS Artifact e o Organizations, ou se remover a conta-membro da organização.

Embora seja possível excluir ou modificar essa função removendo a conta-membro da organização, não recomendamos fazer isso.

Modificar a função não é recomendado porque pode causar problemas de segurança, como confused deputy entre serviços. Para saber mais sobre a proteção contra o ataque “confused deputy”, consulte Prevenção contra o ataque “Confused deputy” em todos os serviços no Guia do usuário do AWS Artifact .

- `AWSServiceRoleForArtifact`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pela AWS Artifact concedem acesso aos seguintes diretores de serviço:

- `artifact.amazonaws.com`

## Habilitar o acesso confiável no AWS Artifact

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode ativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando ou chamando uma operação de API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

2. Na página Services (Serviços), localize a linha para o AWS Artifact, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Artifact que agora ele pode habilitar esse serviço usando seu console para trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitá-lo AWS Artifact como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Ativar AWSServiceAccess

## Desabilitar o acesso confiável no AWS Artifact

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com AWS Artifact.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

AWS Artifact requer acesso confiável AWS Organizations para trabalhar com os acordos da organização. Se você desabilitar o acesso confiável usando AWS Organizations enquanto estiver

usando AWS Artifact os contratos da organização, ele deixará de funcionar porque não pode acessar a organização. Todos os contratos organizacionais que você aceita AWS Artifact permanecem, mas não podem ser acessados por AWS Artifact. O AWS Artifact papel que AWS Artifact cria permanece. Se você reabilitar o acesso confiável, o AWS Artifact continuará operando como antes, sem que você precise reconfigurar o serviço.

Uma conta independente removida de uma organização não tem mais acesso a qualquer contrato da organização.

Você pode desativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando do Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS Artifact e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for administrador do Only AWS Organizations, informe ao administrador AWS Artifact que agora ele pode desativar esse serviço usando o console ou as ferramentas para não trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável a serviços:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar AWS Artifact como um serviço confiável com Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal artifact.amazonaws.com
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Desativar AWSServiceAccess

## AWS Audit Manager e AWS Organizations

O AWS Audit Manager ajuda a auditar continuamente o uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com os regulamentos e padrões do setor. O Audit Manager automatiza a coleta de evidências para tornar mais fácil avaliar se suas políticas, procedimentos e atividades estão funcionando de modo eficaz. Quando é hora de uma auditoria, o Audit Manager ajuda você a gerenciar as revisões de seus controles pelas partes interessadas e ajuda a criar relatórios prontos para auditoria com muito menos esforço manual.

Quando você integra o Audit Manager ao AWS Organizations, pode coletar evidências de uma fonte mais ampla, incluindo várias Contas da AWS de sua organização dentro do escopo de suas avaliações.

Para obter mais informações, consulte Enable AWS Organizations (Habilitar organizações da AWS) no Guia do usuário do Audit Manager.

Use as informações a seguir para ajudá-lo a integrar o AWS Audit Manager ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Audit Manager realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o Audit Manager e o Organizations, ou se remover a conta-membro da organização.

Para obter mais informações sobre como o Audit Manager usa essa função, consulte Uso de funções vinculadas a serviço no Guia do usuário do AWS Audit Manager.

- `AWSServiceRoleForAuditManager`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Audit Manager concedem acesso às seguintes entidades de serviço primárias:

- `auditmanager.amazonaws.com`

## Para habilitar o acesso confiável com o Audit Manager

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

O Audit Manager requer acesso confiável ao AWS Organizations para que você possa designar uma conta-membro como administrador delegado de sua organização.

Você pode habilitar o acesso confiável usando o console do AWS Audit Manager ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Audit Manager para habilitar a integração com o Organizations. Isso permite que o AWS Audit Manager execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Audit Manager. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Audit Manager, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando o console do Audit Manager

Para obter instruções sobre como habilitar o acesso confiável, consulte Configuração no Guia do usuário do AWS Audit Manager.

> **Note**
>
> Se você configurar um administrador delegado usando o console do AWS Audit Manager, o AWS Audit Manager habilita automaticamente o acesso confiável para você.

Você pode habilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para habilitar o acesso confiável a serviços usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Audit Manager como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: EnableAWSServiceAccess

## Para desabilitar o acesso confiável com o Audit Manager

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador na conta de gerenciamento do AWS Organizations pode desabilitar acesso confiável com o AWS Audit Manager.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Audit Manager como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

## Habilitar uma conta de administrador delegado para o Audit Manager

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e as funções dessa conta podem realizar ações administrativas para o Audit Manager que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Audit Manager.

> **Permissões mínimas**
>
> Apenas um usuário ou perfil na conta de gerenciamento do Organizations com a seguinte permissão pode configurar uma conta-membro como administrador delegado para o Audit Manager na organização:
> `audit-manager:RegisterAccount`

Para obter instruções sobre como habilitar uma conta de administrador delegado para o Audit Manager, consulte Configuração no Guia do usuário do AWS Audit Manager.

Se você configurar um administrador delegado usando o console do AWS Audit Manager, o Audit Manager habilitará automaticamente o acesso confiável para você.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, poderá usar os seguintes comandos:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK: chame a operação `RegisterAccount` e forneça `delegatedAdminAccount` como um parâmetro para delegar a conta de administrador.

## AWS Backup e AWS Organizations

AWS Backup é um serviço que permite gerenciar e monitorar os trabalhos do AWS Backup em sua organização. Usando o AWS Backup, se você fizer login como usuário na conta de gerenciamento da organização, é possível habilitar proteção e monitoramento de backup em toda a organização. Isso ajuda a alcançar a conformidade usando políticas de backup para aplicar planos do AWS Backup centralmente a recursos em todas as contas em sua organização. O uso conjunto de AWS Backup e AWS Organizations pode oferecer os seguintes benefícios:

Proteção

Você pode habilitar o tipo de política de backup em sua organização e criar políticas de backup para anexar à raiz, UOs ou contas da organização. Uma política de backup combina um plano do AWS Backup com os outros detalhes necessários para aplicar o plano automaticamente às suas contas. As políticas que estão diretamente vinculadas a uma conta são mescladas com as políticas herdadas da raiz da organização e todas as UOs de nível superior para criar uma política efetiva que se aplica à conta. A política inclui o ID de uma função do IAM que tem permissões para executar o AWS Backup nos recursos de suas contas. O AWS Backup usa a função do IAM para executar o backup em seu nome, como especificado pelo plano de backup na política em vigor.

Monitoramento

Quando habilita o acesso confiável para o AWS Backup na sua organização, você pode usar o console do AWS Backup para ver os detalhes sobre os trabalhos de backup, restauração e cópia em qualquer das contas de sua organização. Para obter mais informações, consulte Monitorar trabalhos de backup no Guia de desenvolvedor do AWS Backup.

Para obter mais informações sobre o AWS Backup, consulte o Guia do desenvolvedor do AWS Backup.

Use as informações a seguir para ajudá-lo a integrar o AWS Backup ao AWS Organizations.

## Habilitar o acesso confiável no AWS Backup

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Backup ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Backup para habilitar a integração com o Organizations. Isso permite que o AWS Backup execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Backup. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Backup, não é necessário concluir estas etapas.

Para habilitar acesso confiável usando o AWS Backup, consulte Habilitar backup em várias Contas da AWS no Guia do desenvolvedor do AWS Backup.

## Desabilitar o acesso confiável no AWS Backup

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

O AWS Backup requer acesso confiável com o AWS Organizations para habilitar o monitoramento de trabalhos de backup, restauração e cópia nas contas de sua organização. Se você desativar o acesso confiável do AWS Backup, perderá a capacidade de exibir trabalhos fora da conta atual. A função do AWS Backup que o AWS Backup cria permanece. Se você reabilitar o acesso confiável mais tarde, o AWS Backup continuará operando como antes, sem que você precise reconfigurar o serviço.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Backup como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

### Como habilitar uma conta de administrador delegado para o AWS Backup

Consulte Administrador delegado no Guia do desenvolvedor do AWS Backup.

## AWS Billing and Cost Management e AWS Organizations

AWS Billing and Cost Management fornece um conjunto de recursos para ajudá-lo a configurar seu faturamento, recuperar e pagar faturas e analisar, organizar, planejar e otimizar seus custos. Ao usar o Billing and Cost Management AWS Organizations , você permite que os dados de alocação de custos divididos AWS Organizations recuperem informações, se aplicável, e coletem dados de telemetria para os serviços de dados de alocação de custos divididos pelos quais você optou.

Use as informações a seguir para ajudá-lo a se integrar AWS Billing and Cost Management com AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Billing and Cost Management realize operações suportadas nas contas da sua organização em sua organização.

Você pode excluir ou modificar essa função somente se desativar o acesso confiável entre Billing and Cost Management and Organizations, ou se remover a conta do membro da organização.

Para obter mais informações, consulte Permissões de função vinculada ao serviço para Billing and Cost Management no Guia do usuário do Billing and Cost Management.

- `AWSServiceRoleForSplitCostAllocationData`

### Princípios de serviço usados pelo Billing and Cost Management

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Billing and Cost Management concedem acesso às seguintes entidades de serviço:

O Billing and Cost Management usa `billing-cost-management.amazonaws.com` o serviço principal.

### Habilitando o acesso confiável com o Billing and Cost Management

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Com o acesso confiável habilitado por meio da conta de gerenciamento, os clientes podem aproveitar o recurso de dados de alocação de custos divididos em Billing and Cost Management. Quando os clientes habilitam dados de alocação de custos divididos para o Amazon Elastic Kubernetes Service com o Amazon Managed Service for Prometheus, o acesso confiável é invocado para criar funções vinculadas a serviços para todas as contas membros da organização. Isso permite dividir os dados de alocação de custos para coletar dados de telemetria dos espaços de trabalho do Amazon Managed Service for Prometheus dos clientes e realizar a alocação de custos com base nessas métricas.

Você pode ativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando ou chamando uma operação de API em um dos AWS SDKs.

### AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Billing and Cost Management, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Billing and Cost Management que agora ele pode habilitar esse serviço usando seu console para trabalhar com ele AWS Organizations.

### AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitá-lo AWS Billing and Cost Management como um serviço confiável com Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Ativar AWSServiceAccess

### Desativação do acesso confiável

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desativar o acesso confiável executando um AWS CLI comando Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável a serviços:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar AWS Billing and Cost Management como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSServiceAccess

## AWS CloudFormation StackSets e AWS Organizations

O AWS CloudFormation StackSets permite criar, atualizar ou excluir pilhas em várias Contas da AWS e Regiões da AWS com uma única operação. A integração do StackSets com o AWS Organizations permite que você crie conjuntos de pilhas com permissões gerenciadas pelo serviço, usando uma função vinculada ao serviço que tenha a permissão relevante em cada conta-membro. Isso permite implantar instâncias de pilha em todas as contas-membro de sua organização. Você não tem que criar as funções do AWS Identity and Access Management necessárias; o StackSets cria a função do IAM em cada conta-membro em seu nome.

Você também pode optar por habilitar implantações automáticas nas contas que serão adicionadas à sua organização no futuro. Com a implantação automática ativada, as funções e a implantação de

instâncias associadas do conjunto de pilhas são adicionadas automaticamente a todas as contas adicionadas no futuro a essa OU.

Com acesso confiável entre o StackSets e o Organizations habilitado, a conta de gerenciamento tem permissões para criar e gerenciar conjuntos de pilhas para sua organização. A conta de gerenciamento pode registrar até cinco contas-membro como administradores delegados. Com o acesso confiável habilitado, os administradores delegados também têm permissões para criar e gerenciar conjuntos de pilhas para sua organização. Os conjuntos de pilha com permissões gerenciadas por serviço são criados na conta de gerenciamento, incluindo conjuntos de pilha criados por administradores delegados.

> **Important**
>
> Os administradores delegados têm permissões completas para implantar em contas em sua organização. A conta de gerenciamento não pode limitar as permissões de administrador delegado para implantar em OUs específicas ou para executar operações específicas de conjunto de pilha.

Para obter mais informações sobre como integrar o StackSets ao Organizations, consulte Trabalhar com o AWS CloudFormation StackSets no Guia do usuário do AWS CloudFormation.

Use as informações a seguir para ajudá-lo a integrar o AWS CloudFormation StackSets ao AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que os Stacksets do AWS CloudFormation realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o AWS CloudFormation e o Organizations, ou se remover a conta-membro da organização.

- Gerenciamento de contas: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

Para criar a função vinculada a serviço `AWSServiceRoleForCloudFormationStackSetsOrgMember` para as contas-membro em sua

organização, primeiro é necessário criar um conjunto de pilhas na conta de gerenciamento. Isso cria uma instância de conjunto de pilhas, que então cria a função nas contas-membro.

- Contas-membro: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Para obter mais detalhes sobre a criação de conjuntos de pilhas, consulte Trabalhar com o AWS CloudFormation StackSets no Guia do usuário do AWS CloudFormation.

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo AWS CloudFormation Stacksets concedem acesso às seguintes entidades primárias de serviço:

- Gerenciamento de contas: `stacksets.cloudformation.amazonaws.com`

  Você só pode modificar ou excluir essa função se o acesso confiável entre o StackSets e o Organizations estiver desabilitado.
- Contas-membro: `member.org.stacksets.cloudformation.amazonaws.com`

  Você só pode modificar ou excluir essa função se o acesso confiável entre o StackSets e o Organizations for desabilitado ou se a conta for removida da organização ou da unidade organizacional (UO) em questão.

## Habilitar o acesso confiável no AWS CloudFormation Stacksets

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Somente um administrador da conta de gerenciamento da organização tem permissões para habilitar o acesso confiável com outro serviço da AWS. Você pode habilitar o acesso confiável usando o console do AWS CloudFormation ou o console do Organizations.

Você pode habilitar o acesso confiável usando apenas o AWS CloudFormation StackSets.

Para habilitar o acesso confiável usando o console do AWS CloudFormation Stacksets, consulte Habilitar o acesso confiável no AWS Organizations no Guia do usuário do AWS CloudFormation.

## Desabilitar o acesso confiável no AWS CloudFormation Stacksets

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador em uma conta de gerenciamento da organização tem permissões para desabilitar o acesso confiável com outro serviço da AWS. Você pode desabilitar o acesso confiável apenas usando o console do Organizations. Se você desabilitar o acesso confiável com o Organizations enquanto estiver usando o StackSets, todas as instâncias de pilha criadas anteriormente serão mantidas. No entanto, os conjuntos de pilhas implantados usando permissões da função vinculada ao serviço não podem mais realizar implantações em contas gerenciadas pelo Organizations.

Você pode desabilitar o acesso confiável usando o console do AWS CloudFormation ou o console do Organizations.

> **Important**
>
> Se você desabilitar o acesso confiável programaticamente (P. EX., com a AWS CLI ou com uma API), lembre-se de que isso removerá a permissão. É melhor desabilitar o acesso confiável com o console do AWS CloudFormation.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS CloudFormation StackSets e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).

5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS CloudFormation StackSets que agora ele pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS CloudFormation StackSets como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

### Habilitar uma conta de administrador delegado para o AWS CloudFormation Stacksets

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e as funções dessa conta podem realizar ações administrativas para o AWS CloudFormation Stacksets que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do AWS CloudFormation Stacksets.

Para obter instruções sobre como designar uma conta-membro como administrador delegado do AWS CloudFormation StackSets na organização, consulte Registrar um administrador delegado no Guia do usuário do AWS CloudFormation.

## AWS CloudTrail e AWS Organizations

AWS CloudTrail é um AWS serviço que ajuda você a viabilizar a governança, a conformidade e a auditoria operacional e de risco do seu Conta da AWS. Usando AWS CloudTrail, um usuário em uma conta de gerenciamento pode criar uma trilha da organização que registra todos os eventos de

todos Contas da AWS nessa organização. As trilhas da organização são aplicadas automaticamente a todas as contas-membro da organização. As contas-membro podem ver a trilha da organização, mas não pode modificá-la ou excluí-la. Por padrão, as contas-membro não têm acesso aos arquivos de log da trilha da organização no bucket do Amazon S3. Isso ajuda você a aplicar e impor sua estratégia de registro de eventos em log de modo uniforme em todas as contas de sua organização.

Para obter informações consulte Criar uma trilha para uma organização no Guia do usuário doAWS CloudTrail .

Use as informações a seguir para ajudá-lo a se integrar AWS CloudTrail com AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite CloudTrail realizar operações suportadas nas contas da sua organização em sua organização.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o CloudTrail e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForCloudTrail`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pela CloudTrail concedem acesso aos seguintes diretores de serviço:

- `cloudtrail.amazonaws.com`

## Habilitar o acesso confiável no CloudTrail

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Se você habilitar o acesso confiável criando uma trilha no AWS CloudTrail console, o acesso confiável será configurado automaticamente para você (recomendado). Você também pode ativar o acesso confiável usando o AWS Organizations console. Você deve entrar com sua conta AWS Organizations de gerenciamento para criar uma trilha organizacional.

Se você optar por criar uma trilha organizacional usando a AWS CLI ou a AWS API, deverá configurar manualmente o acesso confiável. Para obter mais informações, consulte Habilitar CloudTrail como um serviço confiável AWS Organizationsno GuiaAWS CloudTrail do usuário.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS CloudTrail console ou as ferramentas para permitir a integração com o Organizations.

Você pode habilitar o acesso confiável executando um AWS CLI comando Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para habilitar o acesso confiável a serviços usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitá-lo AWS CloudTrail como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Ativar AWSServiceAccess

## Desabilitar o acesso confiável no CloudTrail

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

AWS CloudTrail requer acesso confiável AWS Organizations para trabalhar com trilhas organizacionais e armazenamentos de dados de eventos da organização. Se você desativar o acesso confiável usando AWS Organizations enquanto estiver usando AWS CloudTrail, todas

as trilhas da organização para contas de membros serão excluídas porque não é CloudTrail possível acessar a organização. Todas as trilhas de organização da conta de gerenciamento e os armazenamentos de dados de eventos da organização são convertidos em trilhas no nível da conta e armazenamentos de dados de eventos. A `AWSServiceRoleForCloudTrail` função criada para integração entre CloudTrail e AWS Organizations permanece na conta. Se você reativar o acesso confiável, não CloudTrail tomará medidas em trilhas e armazenamentos de dados de eventos existentes. A conta de gerenciamento deve atualizar todas as trilhas no nível da conta e os armazenamentos de dados de eventos para aplicá-los à organização.

Para converter uma trilha em nível de conta ou armazenamento de dados de eventos em uma trilha da organização ou armazenamento de dados de eventos da organização, faça o seguinte:

- No CloudTrail console, atualize o armazenamento de dados da trilha ou do evento e escolha a opção Habilitar para todas as contas na minha organização.
- A partir do AWS CLI, faça o seguinte:
  - Para atualizar uma trilha, execute o update-trailcomando e inclua o `--is-organization-trail` parâmetro.
  - Para atualizar um armazenamento de dados de eventos, execute o update-event-data-storecomando e inclua o `--organization-enabled` parâmetro.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com AWS CloudTrail. Você pode desativar o acesso confiável somente com as ferramentas do Organizations, usando o AWS Organizations console, executando um comando da AWS CLI do Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

Você pode desativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando do Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS CloudTrail e escolha o nome do serviço.

3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for administrador do Only AWS Organizations, informe ao administrador AWS CloudTrail que agora ele pode desativar esse serviço usando o console ou as ferramentas para não trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável a serviços:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar AWS CloudTrail como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSServiceAccess

## Habilitando uma conta de administrador delegado para CloudTrail

Ao usar CloudTrail com Organizations, você pode registrar qualquer conta dentro da organização para atuar como administrador CloudTrail delegado para gerenciar as trilhas e os armazenamentos de dados de eventos da organização em nome da organização. Um administrador delegado é uma conta membro em uma organização que pode realizar as mesmas tarefas administrativas da conta de gerenciamento. CloudTrail

> **Permissões mínimas**
>
> Somente um administrador na conta de gerenciamento da Organizations pode registrar um administrador delegado para CloudTrail.

Você pode registrar uma conta de administrador delegado usando o CloudTrail console ou usando a operação Organizations `RegisterDelegatedAdministrator` CLI ou SDK. Para registrar um administrador delegado usando o CloudTrail console, consulte Adicionar um administrador CloudTrail delegado.

### Desabilitando um administrador delegado para CloudTrail

Somente um administrador na conta de gerenciamento da Organizations pode remover um administrador delegado do. CloudTrail Você pode remover o administrador delegado usando o CloudTrail console ou usando a operação Organizations `DeregisterDelegatedAdministrator` CLI ou SDK. Para obter informações sobre como remover um administrador delegado usando o CloudTrail console, consulte Remover um administrador CloudTrail delegado.

## AWS Compute Optimizer e AWS Organizations

O AWS Compute Optimizer é um serviço que analisa as métricas de configuração e utilização dos seus recursos da AWS. Exemplos de recursos incluem instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e dos grupos do Auto Scaling. O Compute Optimizer informa se seus recursos estão em condições ideais e gera recomendações de otimização para reduzir o custo e melhorar a performance de suas cargas de trabalho. Para obter mais informações sobre o Compute Optimizer, consulte o AWS Compute OptimizerGuia do usuário do .

Use as informações a seguir para ajudá-lo a integrar o AWS Compute Optimizer ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Compute Optimizer realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o Compute Optimizer e o Organizations, ou se você remover a conta-membro da organização.

- `AWSServiceRoleForComputeOptimizer`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Compute Optimizer concedem acesso às seguintes entidades de serviço primárias:

- `compute-optimizer.amazonaws.com`

## Habilitar o acesso confiável no Compute Optimizer

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Compute Optimizer ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Compute Optimizer para habilitar a integração com o Organizations. Isso permite que o AWS Compute Optimizer execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Compute Optimizer. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Compute Optimizer, não é necessário concluir estas etapas.

### Para habilitar o acesso confiável usando o console do Compute Optimizer

Você deve fazer login no console do Compute Optimizer usando a conta de gerenciamento de sua organização. Aceite a inclusão em nome de sua organização seguindo as instruções em Inclusão da sua conta no Guia do usuário do AWS Compute Optimizer.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Compute Optimizer, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Compute Optimizer que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Compute Optimizer como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no Compute Optimizer

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador na conta de gerenciamento do AWS Organizations pode desabilitar acesso confiável com o AWS Compute Optimizer.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Compute Optimizer como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

## Habilitar uma conta de administrador delegado para o Compute Optimizer

Quando você designa uma conta-membro como administrador delegado da organização, os usuários e as funções da conta designada podem gerenciar os metadados da Conta da AWS de outras contas-membro na organização. Se você não habilitar uma conta de administrador delegado, essas tarefas só poderão ser executadas pela conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento de detalhes da sua conta.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como administrador delegado do Compute Optimizer na organização

Para obter instruções sobre como habilitar uma conta de administrador delegado para o Compute Optimizer, consulte https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html no Guia do usuário do AWS Compute Optimizer.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, poderá usar os seguintes comandos:

- AWS CLI:

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

- AWS SDK: chame a operação `RegisterDelegatedAdministrator` do Organizations e o número de ID da conta-membro e identifique a entidade principal do serviço de conta `account.amazonaws.com` como parâmetros.

### Desabilitar uma conta de administrador delegado para o Compute Optimizer

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para o Compute Optimizer.

Para desabilitar a conta de administrador delegado do Compute Optimizer usando o console do Compute Optimizer, consulte https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html no Guia do usuário do AWS Compute Optimizer.

Para remover um administrador delegado usando a AWS AWS CLI, consulte deregister-delegated-administrator na Referência de comandos da AWS AWS CLI.

## AWS Config e AWS Organizations

A agregação de dados de várias regiões e contas no AWS Config permite agregar dados do AWS Config de várias contas e regiões da Regiões da AWS em uma única conta. A agregação de dados de várias regiões e várias contas é útil para os administradores da TI central monitorarem a conformidade das várias Contas da AWS da empresa. Um agregador é um tipo de recurso do AWS Config que coleta dados do AWS Config de várias contas e regiões de origem. Crie um agregador na região onde você deseja ver os dados do AWS Config agregados. Ao criar um agregador, você pode

optar por adicionar IDs de contas individuais ou sua organização. Para obter mais informações sobre o AWS Config, consulte o AWS ConfigGuia do desenvolvedor do .

Você também pode usar APIs do AWS Config para gerenciar regras do AWS Config em todas as Contas da AWS de sua organização. Para obter mais informações, consulte Habilitar regras do AWS Config em todas as contas de sua organização no Guia do desenvolvedor do AWS Config.

Use as informações a seguir para ajudá-lo a integrar o AWS Config ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita acesso confiável. Essa função permite que o AWS Config realize as operações suportadas nas contas de sua organização.

- `AWSServiceRoleForConfig`

Essa função é criada quando você habilita o AWS Config em sua organização criando um agregador de várias contas. O AWS Config solicita que você selecione ou crie uma função e forneça o nome. O nome não é gerado automaticamente.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o AWS Config e o Organizations, ou se remover a conta-membro da organização.

### Habilitar o acesso confiável no AWS Config

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Config ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Config para habilitar a integração com o Organizations. Isso permite que o AWS Config execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Config. Para obter mais informações, consulte esta nota.

Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Config, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando o console do AWS Config

Para habilitar o acesso confiável com o AWS Organizations usando o AWS Config, crie um agregador de várias contas e adicione a organização. Para obter informações sobre como configurar um agregador de várias contas, consulte Configuração de um agregador usando o console, no Guia do desenvolvedor do AWS Config.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Config, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Config que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

Você pode executar o comando a seguir para habilitar o AWS Config como um serviço confiável com o Organizations.

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

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no AWS Config

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Config como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

# Hub de Otimização de Custos da AWS e AWS Organizations

Hub de Otimização de Custos da AWS é um recurso de AWS Billing and Cost Management que ajuda você a consolidar e priorizar as recomendações de otimização de custos em AWS suas contas AWS e regiões, para que você possa aproveitar ao máximo seus gastos. AWS Ao usar o Cost Optimization Hub, AWS Organizations você pode facilmente identificar, filtrar e agregar recomendações de otimização de AWS custos em todas as contas e AWS regiões membros do Organizations.

Para obter mais informações, consulte Cust Optimization Hub no Guia AWS Cost Management do usuário.

Use as informações a seguir para ajudá-lo a se integrar Hub de Otimização de Custos da AWS com AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Cost Optimization Hub execute operações suportadas nas contas de sua organização em sua organização.

Você pode excluir ou modificar essa função somente se desativar o acesso confiável entre o Cost Optimization Hub e Organizations, ou se remover a conta membro da organização.

Para obter mais informações, consulte Permissões de função vinculada ao serviço para o Cost Optimization Hub no Guia do AWS Cost Management usuário.

- `AWSServiceRoleForCostOptimizationHub`

## Princípios de serviço usados pelo Cost Optimization Hub

O Cost Optimization Hub usa o `cost-optimization-hub.bcm.amazonaws.com` serviço principal.

## Habilitando acesso confiável com o Cost Optimization Hub

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Quando você opta por usar a conta de gerenciamento da sua organização e inclui todas as contas dos membros da organização, o acesso confiável ao Cost Optimization Hub é habilitado automaticamente na conta da sua organização.

Você pode ativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando ou chamando uma operação de API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o Hub de Otimização de Custos da AWS, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for administrador de somente AWS Organizations, informe ao administrador Hub de Otimização de Custos da AWS que agora ele pode habilitar esse serviço usando seu console para trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitá-lo Hub de Otimização de Custos da AWS como um serviço confiável com Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Ativar AWSServiceAccess

## Desativação do acesso confiável

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

> **Important**
>
> Se você desativar o acesso confiável ao Cost Optimization Hub depois de se inscrever, o Cost Optimization Hub negará o acesso às recomendações para as contas membros da sua organização. Além disso, as contas dos membros da organização não estão cadastradas no Cost Optimization Hub. Saiba mais em Cost Optimization Hub and Organizations Trusted Access no Guia AWS Cost Management do Usuário.

Você pode desativar o acesso confiável executando um AWS CLI comando Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável a serviços:

- AWS CLI: disable-aws-service-access

Você pode executar o comando a seguir para desabilitar Hub de Otimização de Custos da AWS como um serviço confiável com Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Desativar AWSServiceAccess

## AWS Control Tower e AWS Organizations

O AWS Control Tower oferece uma maneira simples de configurar e governar um ambiente de várias contas da AWS, seguindo as práticas recomendadas prescritivas. A orquestração do AWS Control Tower amplia os recursos de AWS Organizations. O AWS Control Tower aplica controles preventivos e de detecção (barreiras de proteção) para ajudar a evitar que suas organizações e contas divirjam das práticas recomendadas (drift).

A orquestração do AWS Control Tower amplia os recursos de AWS Organizations.

Para obter mais informações, consulte o Guia do usuário do AWS Control Tower.

Use as informações a seguir para ajudá-lo a integrar o AWS Control Tower ao AWS Organizations.

### Funções necessárias para a integração

A função `AWSControlTowerExecution` deve estar presente em todas as contas cadastradas. Ela permite que o AWS Control Tower gerencie suas contas individuais e relate informações sobre elas nas contas de auditoria e registro em log.

Para saber mais sobre as funções usadas pelo AWS Control Tower, consulte How AWS Control Tower works with roles to create and manage accounts (Como o trabalha com perfis para criar e gerenciar contas) e Using Identity-Based Policies (IAM Policies) for AWS Control Tower (Uso de políticas baseadas em identidade (políticas do IAM) para o ).

### Entidades principais de serviço usadas pelo AWS Control Tower

O AWS Control Tower usa a entidade principal de serviço `controltower.amazonaws.com`.

### Habilitar o acesso confiável no AWS Control Tower

O AWS Control Tower usa acesso confiável para detectar desvios de controles preventivos e para rastrear alterações na conta e na UO que causam desvios.

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando apenas as ferramentas do Organizations.

Para habilitar o acesso confiável no console do Organizations, escolha **`Enable access`** próximo a AWS Control Tower.

Você pode habilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para habilitar o acesso confiável a serviços usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Control Tower como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no AWS Control Tower

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

> **Important**
>
> A desativação do AWS Control Tower acesso confiável causa desvio na sua zona de AWS Control Tower pouso. A única maneira de corrigir o desvio é usar o reparo AWS Control Tower da Landing Zone. Reativar o acesso confiável nas organizações não resolve o problema. Saiba mais sobre desvio noAWS Control Tower guia do usuário.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Control Tower como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

## Amazon Detective e AWS Organizations

O Amazon Detective usa seus dados de log para gerar visualizações que permitem analisar, investigar e identificar a causa raiz de descobertas de segurança ou atividades suspeitas.

O uso do AWS Organizations permite garantir que o gráfico de comportamento do Detective forneça visibilidade da atividade de todas as contas da sua organização.

Quando você concede acesso confiável ao Detective, o serviço Detective pode reagir automaticamente às alterações na associação à organização. O administrador delegado pode habilitar qualquer conta da organização como uma conta-membro no gráfico de comportamento. O Detective também pode habilitar novas contas-membro da organização. As contas da organização não podem se desassociar do gráfico de comportamento.

Para obter mais informações, consulte Usar o Amazon Detective na organização no Guia de administração do Amazon Detective.

Use as informações a seguir para integrar o Amazon Detective ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Detective realize as operações suportadas nas contas de sua organização.

Você poderá excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o Detective e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForDetective`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Detective concedem acesso às seguintes entidades de serviço primárias:

- `detective.amazonaws.com`

### Para habilitar o acesso confiável com o Detective

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

> **Note**
>
> Quando você designa um administrador delegado para o Amazon Detective, o Detective habilita automaticamente o acesso confiável para o Detective em sua organização.
> O Detective requer acesso confiável ao AWS Organizations para que você possa designar uma conta-membro como administrador delegado desse serviço na sua organização.

Você pode habilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode habilitar o acesso confiável usando o console do AWS Organizations.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o Amazon Detective, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do Amazon Detective que ele agora pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

## Para habilitar o acesso confiável com o Detective

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador na conta de gerenciamento do AWS Organizations pode desabilitar o acesso confiável com o Amazon Detective.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do Amazon Detective e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).

4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do Amazon Detective que ele agora pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

## Habilitar uma conta de administrador delegado do Detective

A conta de administrador delegado do Detective é a conta de administrador de um gráfico de comportamento do Detective. O administrador delegado pode determina quais contas da organização serão habilitadas e desabilitadas como contas-membro nesse gráfico de comportamento. O administrador delegado pode configurar o Detective para habilitar automaticamente novas contas da organização como contas-membro à medida que forem adicionadas à organização. Para obter informações sobre como um administrador delegado gerencia contas da organização, consulte Gerenciar contas da organização como contas-membro no Guia de administração do Amazon Detective.

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado do Detective.

É possível especificar uma conta de administrador delegado via console ou API do Detective ou usando a operação da CLI ou do SDK do Organizations.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como administrador delegado do Detective na organização

Para configurar um administrador delegado usando o console ou a API do Detective, consulte Designar uma conta de administrador do Detective para uma organização no Guia de administração do Amazon Detective.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, poderá usar os seguintes comandos:

- AWS CLI:

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

- AWS SDK: chame a operação `RegisterDelegatedAdministrator` do Organizations e o número de ID da conta-membro e identifique a entidade principal do serviço de conta `account.amazonaws.com` como parâmetros.

### Desabilitar um administrador delegado do Detective

É possível remover a conta de administrador delegado via console ou API do Detective ou usando a operação `DeregisterDelegatedAdministrator` da CLI ou o SDK do Organizations. Para obter informações sobre como remover administrador delegado usando o console ou a API do Detective ou a API do Organizations, consulte Designar uma conta de administrador do Detective para uma organização no Guia de administração do Amazon Detective.

## Amazon DevOps Guru e AWS Organizations

O Amazon DevOps Guru analisa dados operacionais e métricas e eventos de aplicações para identificar comportamentos que se desviam dos padrões operacionais normais. Os usuários são notificados quando o DevOps Guru detecta um problema ou risco operacional.

O uso do DevOps Guru habilita o suporte a várias contas com o AWS Organizations para que você possa designar uma conta-membro para gerenciar insights em toda a organização. Esse administrador delegado pode então visualizar, classificar e filtrar insights de todas as contas dentro de sua organização para desenvolver uma visão holística da integridade de todas as aplicações monitoradas dentro de sua organização sem a necessidade de personalização adicional.

Para obter mais informações, consulte Monitorar contas em toda a organização no Guia do usuário do Amazon DevOps Guru.

Use as informações a seguir para ajudá-lo a integrar o Amazon DevOps Guru ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o DevOps Guru realize as operações suportadas nas contas de sua organização.

Você poderá excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o DevOps Guru e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForDevOpsGuru`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo DevOps Guru concedem acesso às seguintes entidades de serviço principais:

- `devops-guru.amazonaws.com`

Para obter mais informações, consulte Usar funções vinculadas ao serviço para o DevOps Guru, no Guia do usuário do Amazon DevOps Guru.

### Para habilitar o acesso confiável com o DevOps Guru

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

> **Note**
>
> Quando você designa um administrador delegado para o Amazon DevOps Guru, o DevOps Guru habilita automaticamente o acesso confiável para o DevOps Guru na sua organização.
> O DevOps Guru requer acesso confiável ao AWS Organizations para que você possa designar uma conta-membro como administrador delegado desse serviço na sua organização.

> **Important**
>
> É altamente recomendável, sempre que possível, usar o console ou as ferramentas do Amazon DevOps Guru para habilitar a integração com o Organizations. Isso permite que o Amazon DevOps Guru realize qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar

a integração usando as ferramentas fornecidas pelo Amazon DevOps Guru. Para obter mais informações, consulte esta nota.

Você pode habilitar o acesso confiável usando o console do AWS Organizations ou o console do DevOps Guru.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o Amazon DevOps Guru, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do Amazon DevOps Guru que ele agora pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

DevOps Guru console

Para habilitar o acesso confiável ao serviço usando o console do DevOps Guru

1. Faça login como administrador na conta de gerenciamento e abra o console do DevOps Guru: Console do Amazon DevOps Guru
2. Escolha Enable trusted access (Habilitar acesso confiável).

## Para desabilitar o acesso confiável com o DevOps Guru

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador na conta de gerenciamento do AWS Organizations pode desabilitar o acesso confiável com o Amazon DevOps Guru.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do Amazon DevOps Guru e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do Amazon DevOps Guru que ele agora pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

## Habilitar uma conta de administrador delegado para o DevOps Guru

A conta de administrador delegado do DevOps Guru pode ver os dados de insights de todas as contas-membro integradas ao DevOps Guru da organização. Para obter informações sobre como um administrador delegado gerencia contas da organização, consulte Monitorar contas na organização no Guia do usuário do Amazon DevOps Guru.

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado do DevOps Guru.

É possível especificar uma conta de administrador delegado via console do DevOps Guru ou usando a operação `RegisterDelegatedAdministrator` da CLI ou do SDK do Organizations.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como administrador delegado do DevOps Guru na organização

DevOps Guru console

Para configurar um administrador delegado no console do DevOps Guru

1. Faça login como administrador na conta de gerenciamento e abra o console do DevOps Guru: Console do Amazon DevOps Guru
2. Selecione Registrar administrador delegado. Você pode escolher a conta de gerenciamento ou qualquer conta-membro como administrador delegado.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, poderá usar os seguintes comandos:

- AWS CLI:

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

- AWS SDK: chame a operação `RegisterDelegatedAdministrator` do Organizations e o número de ID da conta-membro e identifique a entidade principal do serviço de conta `account.amazonaws.com` como parâmetros.

### Desabilitar um administrador delegado do DevOps Guru

É possível remover a conta de administrador delegado via console do DevOps Guru ou usando a operação `DeregisterDelegatedAdministrator` da CLI ou o SDK do Organizations. Para obter informações sobre como remover um administrador delegado usando o console do DevOps Guru, consulte Monitorar contas na organização no Guia do usuário do Amazon DevOps Guru.

## AWS Directory Service e AWS Organizations

O AWS Directory Service para Microsoft Active Directory, ou o AWS Managed Microsoft AD, permite executar o Microsoft Active Directory (AD) como um serviço gerenciado. O AWS Directory Service facilita a configuração e a execução de diretórios na nuvem da AWS ou a conexão de seus recursos existentes da AWS com um Microsoft Active Directory existente no local. O AWS Managed Microsoft AD também se integra perfeitamente com o AWS Organizations para permitir o compartilhamento

sem falhas de diretórios entre várias Contas da AWS e qualquer VPC em uma região. Para obter mais informações, consulte o Guia do administrador do AWS Directory Service.

Use as informações a seguir para ajudá-lo a integrar o AWS Directory Service ao AWS Organizations.

## Habilitar o acesso confiável no AWS Directory Service

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Directory Service ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Directory Service para habilitar a integração com o Organizations. Isso permite que o AWS Directory Service execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Directory Service. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Directory Service, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando o console do AWS Directory Service

Para compartilhar um diretório, o que habilita automaticamente o acesso confiável, consulte Compartilhar seu diretório no Guia de administração do AWS Directory Service. Para obter instruções detalhadas, consulte o tutorial: Compartilhamento de seu AWS Managed Microsoft AD Directory.

Você pode habilitar o acesso confiável usando o console do AWS Organizations.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Directory Service, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Directory Service que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

## Desabilitar o acesso confiável no AWS Directory Service

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Se você desabilitar o acesso confiável usando o AWS Organizations enquanto você estiver usando o AWS Directory Service, todos os diretórios compartilhados anteriormente continuarão funcionando normalmente. No entanto, você não poderá mais compartilhar novos diretórios dentro da organização até ter reabilitado o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS Directory Service e escolha o nome do serviço.

3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Directory Service que agora ele pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

## AWS Firewall Manager e AWS Organizations

O AWS Firewall Manager é um serviço de gerenciamento de segurança usado para configurar e gerenciar centralmente regras de firewall e outras proteções em todas as Contas da AWS e aplicativos na organização. Usando o Firewall Manager, é possível implementar regras do AWS WAF, criar proteções do AWS Shield Advanced, configurar e auditar grupos de segurança do Amazon Virtual Private Cloud (Amazon VPC) e implantar AWS Network Firewalls. Use o Firewall Manager para configurar suas regras de firewall apenas uma vez e aplique-as automaticamente em todas as contas e recursos de sua organização, mesmo quando novos recursos e contas forem adicionados. Para obter mais informações sobre o AWS Firewall Manager, consulte o Guia do desenvolvedor do AWS Firewall Manager.

Use as informações a seguir para ajudá-lo a integrar o AWS Firewall Manager ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Firewall Manager realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o Firewall Manager e o Organizations, ou se você remover a conta-membro da organização.

- `AWSServiceRoleForFMS`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções

vinculadas ao serviço usadas pelo Firewall Manager concedem acesso às seguintes entidades de serviço primárias:

- `fms.amazonaws.com`

## Habilitar o acesso confiável no Firewall Manager

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Firewall Manager ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Firewall Manager para habilitar a integração com o Organizations. Isso permite que o AWS Firewall Manager execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Firewall Manager. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Firewall Manager, não é necessário concluir estas etapas.

Você deve fazer login com sua conta de gerenciamento do AWS Organizations e configurar uma conta da organização como a conta de administrador do AWS Firewall Manager. Para obter mais informações, consulte Definir a conta de administrador do AWS Firewall Manager no Guia do desenvolvedor do AWS Firewall Manager.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Firewall Manager, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Firewall Manager que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Firewall Manager como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no Firewall Manager

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando as ferramentas do AWS Firewall Manager ou do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Firewall Manager para desabilitar a integração com o Organizations. Isso permite que o AWS Firewall Manager realize qualquer limpeza necessária, como excluir recursos ou funções de acesso que não são mais necessários para o serviço. Continue com estas etapas apenas se você não puder desabilitar a integração usando as ferramentas fornecidas pelo AWS Firewall Manager.
>
> Se você desabilitar o acesso confiável usando o console ou as ferramentas do AWS Firewall Manager, não é necessário concluir estas etapas.

Para desabilitar acesso confiável usando o console do Firewall Manager

Você pode alterar ou revogar a conta de administrador do AWS Firewall Manager seguindo as instruções em Designação de outra conta como a conta de administrador do AWS Firewall Manager no Guia do desenvolvedor do AWS Firewall Manager.

Se revogar a conta de administrador, você deve fazer login na conta de gerenciamento do AWS Organizations e definir uma nova conta de administrador para o AWS Firewall Manager.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS Firewall Manager e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).

4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Firewall Manager que agora ele pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Firewall Manager como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

## Habilitar uma conta de administrador delegado para o Firewall Manager

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e funções dessa conta podem executar ações administrativas para o Firewall Manager que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Firewall Manager.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como administrador delegado para o Firewall Manager na organização.

Para obter instruções sobre como designar uma conta-membro como administrador do Firewall Manager para a organização, consulte Definir a Conta do administrador do AWS Firewall Manager no Guia do desenvolvedor do AWS Firewall Manager.

## Amazon GuardDuty e AWS Organizations

O Amazon GuardDuty é um serviço contínuo de monitoramento de segurança que analisa e processa uma variedade de fontes de dados, usando feeds de inteligência sobre ameaças e machine learning para identificar atividades inesperadas e potencialmente não autorizadas e maliciosas dentro do seu ambiente da AWS. Isso pode incluir problemas como escalonamentos de privilégios, uso de credenciais expostas, comunicação com endereços IP, URLs ou domínios mal-intencionados ou presença de malware nas instâncias e workloads de contêiner do Amazon Elastic Compute Cloud.

Você pode ajudar a simplificar o gerenciamento do GuardDuty usando o Organizations para gerenciar o GuardDuty em todas as contas de sua organização.

Para obter mais informações, consulte Gerenciar contas do GuardDuty com o AWS Organizations no Guia do usuário do Amazon GuardDuty

Use as informações a seguir para ajudá-lo a integrar o Amazon GuardDuty ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

As funções vinculadas ao serviço a seguir são criadas automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Elas permitem que o GuardDuty realize as operações suportadas nas contas de sua organização. Você só pode excluir uma função se desabilitar o acesso confiável entre o GuardDuty e o Organizations, ou se você remover a conta-membro da organização.

- A função vinculada ao serviço `AWSServiceRoleForAmazonGuardDuty` é criada automaticamente em contas que integraram o GuardDuty com o Organizations. Para obter mais informações, consulte Gerenciar contas do GuardDuty com o Organizations no Guia do usuário do Amazon GuardDuty
- A função vinculada ao serviço `AmazonGuardDutyMalwareProtectionServiceRolePolicy` é automaticamente criada nas contas que ativaram GuardDuty Malware Protection. Para obter mais informações, consulte Permissões da função vinculada ao serviço para o GuardDuty Malware Protection no Guia do usuário do Amazon GuardDuty

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

- `guardduty.amazonaws.com`, usado pela função vinculada ao serviço `AWSServiceRoleForAmazonGuardDuty`.
- `malware-protection.guardduty.amazonaws.com`, usado pela função vinculada ao serviço `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

## Habilitar o acesso confiável no GuardDuty

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando apenas o Amazon GuardDuty.

O Amazon GuardDuty requer acesso confiável ao AWS Organizations para você poder designar uma conta-membro como administrador do GuardDuty para a sua organização. Se você configurar um administrador delegado usando o console do GuardDuty, o GuardDuty habilita automaticamente o acesso confiável para você.

No entanto, se você desejar configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, chame explicitamente a operação EnableAWSServiceAccess e forneça a entidade de serviço primária como um parâmetro. Então, você pode chamar EnableOrganizationAdminAccount para delegar a conta de administrador do GuardDuty.

## Desabilitar o acesso confiável no GuardDuty

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o Amazon GuardDuty como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

### Habilitar uma conta de administrador delegado para o GuardDuty

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e funções dessa conta podem executar ações administrativas para o GuardDuty que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do GuardDuty.

> **Permissões mínimas**
>
> Para obter informações sobre as permissões necessárias para designar uma conta-membro como administrador delegado, consulte Permissões necessárias para designar um administrador delegado no Guia do usuário do Amazon GuardDuty

Para designar uma conta-membro como administrador delegado do GuardDuty

Consulte Designar um administrador delegado e adicionar contas-membro (console) e Designar um administrador delegado e adicionar contas-membro (API)

## AWS Health e AWS Organizations

AWS Health fornece visibilidade contínua do desempenho de seus recursos e da disponibilidade de seus AWS serviços e contas. AWS Health entrega eventos quando seus AWS recursos e serviços são afetados por um problema ou serão afetados por mudanças futuras. Depois de ativar a visualização organizacional, um usuário na conta de gerenciamento da organização pode agregar

AWS Health eventos em todas as contas da organização. A visualização organizacional mostra apenas AWS Health os eventos entregues após a ativação do recurso e os retém por 90 dias.

Você pode ativar a visualização organizacional usando o AWS Health console, o AWS Command Line Interface (AWS CLI) ou a AWS Health API.

Para obter mais informações, consulte Agregação de AWS Health eventos no Guia do AWS Health usuário.

Use as informações a seguir para ajudá-lo a se integrar AWS Health com AWS Organizations.

## Funções vinculadas a serviços para integração

A função `AWSServiceRoleForHealth_Organizations` vinculada ao serviço permite AWS Health realizar operações suportadas nas contas da sua organização em sua organização.

Essa função é criada automaticamente na conta de gerenciamento da sua organização quando você ativa o acesso confiável chamando a operação da EnableHealthServiceAccessForOrganizationAPI. Caso contrário, crie a função usando o AWS Health console, a API ou a CLI, conforme descrito em Criação de uma função vinculada ao serviço no Guia do usuário do IAM.

Você pode excluir ou modificar essa função somente se desativar o acesso confiável entre AWS Health e Organizations ou se remover a conta do membro da organização.

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pela AWS Health concedem acesso aos seguintes diretores de serviço:

- `health.amazonaws.com`

## Habilitar o acesso confiável no AWS Health

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Quando você ativa o recurso de visualização organizacional para AWS Health, o acesso confiável também é habilitado automaticamente para você.

Você pode habilitar o acesso confiável usando o AWS Health console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Health console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Health realizar qualquer configuração necessária, como criar os recursos necessários ao serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Health. Para obter mais informações, consulte esta nota. Se você habilitar o acesso confiável usando o AWS Health console ou as ferramentas, não precisará concluir essas etapas.

Para habilitar o acesso confiável usando o AWS Health console

Você pode ativar o acesso confiável usando AWS Health uma das seguintes opções:

- Use o AWS Health console. Para obter mais informações, consulte Visualização organizacional (console) no Guia do usuário do AWS Health .
- Use a AWS CLI. Para obter mais informações, consulte Visualização organizacional (CLI) no Guia do usuário do AWS Health .
- Chame a operação da API EnableHealthServiceAccessForOrganization.

Você pode habilitar o acesso confiável executando um AWS CLI comando Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para habilitar o acesso confiável a serviços usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitá-lo AWS Health como um serviço confiável com Organizations.

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

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Ativar AWSServiceAccess

## Desabilitar o acesso confiável no AWS Health

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Depois de desativar o recurso de visualização organizacional, AWS Health interrompe a agregação de eventos para todas as outras contas em sua organização. Isso também desabilita o acesso confiável para você automaticamente.

Você pode desativar o acesso confiável usando as AWS Organizations ferramentas AWS Health ou.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Health console ou as ferramentas para desativar a integração com o Organizations. Isso permite AWS Health realizar qualquer limpeza necessária, como excluir recursos ou funções de acesso que não são mais necessários para o serviço. Continue com estas etapas apenas se você não puder desabilitar a integração usando as ferramentas fornecidas pelo AWS Health.
> Se você desabilitar o acesso confiável usando o AWS Health console ou as ferramentas, não precisará concluir essas etapas.

Para desativar o acesso confiável usando o AWS Health console

Você pode desabilitar o acesso confiável com uma das seguintes opções:

- Use o AWS Health console. Para obter mais informações, consulte Desabilitar a visualização organizacional (console) no Guia do usuário do AWS Health .
- Use a AWS CLI. Para obter mais informações, consulte Desabilitar a visualização organizacional (CLI) no Guia do usuário do AWS Health .
- Chame a operação da API DisableHealthServiceAccessForOrganization.

Você pode desativar o acesso confiável executando um AWS CLI comando Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável a serviços:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar AWS Health como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Desativar AWSServiceAccess

## Habilitando uma conta de administrador delegado para AWS Health

Quando você designa uma conta de membro como um administrador delegado para a organização, os usuários e as funções dessa conta podem executar ações administrativas para o AWS Health que, de outra forma, só poderiam ser acionadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do AWS Health.

Para designar uma conta-membro como administrador delegado do  AWS Health

Consulte Registrar um administrador delegado para sua visualização organizacional

Para remover um administrador delegado do  AWS Health

Consulte Remover um administrador delegado da sua visualização organizacional

# Amazon Inspector e AWS Organizations

O Amazon Inspector é um serviço automatizado de gerenciamento de vulnerabilidades que verifica continuamente workloads do Amazon EC2 e do contêiner em busca de vulnerabilidades de software e exposição não intencional da rede.

Usando o Amazon Inspector, você pode gerenciar várias contas associadas por meio de AWS Organizationssimplesmente delegando uma conta de administrador para o Amazon Inspector. O administrador delegado gerencia o Amazon Inspector para a organização e recebe permissões especiais para executar tarefas em nome de sua organização, como:

- Habilitar ou desabilitar verificações para contas-membro
- Vsualizar dados de descoberta agregados de toda a organização
- Criar e gerenciar regras de supressão

Para obter mais informações, consulte Gerenciar várias contas com o AWS Organizations no Guia do usuário do Amazon Inspector.

Use as informações a seguir para integrar o Amazon Inspector ao AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Amazon Inspector realize as operações suportadas nas contas da sua organização.

Você poderá excluir ou modificar essa função somente se desabilitar o acesso confiável entre o Amazon Inspector e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForAmazonInspector2`

Para obter mais informações, consulte Usar funções vinculadas ao serviço com o Amazon Inspector no Guia do usuário do Amazon Inspector.

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções

vinculadas ao serviço usadas pelo Amazon Inspector concedem acesso às seguintes entidades de serviço principais:

- `inspector2.amazonaws.com`

## Para habilitar o acesso confiável com o Amazon Inspector

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

O Amazon Inspector requer acesso confiável ao AWS Organizations para que você possa designar uma conta-membro como administrador delegado desse serviço na sua organização.

Quando você designa um administrador delegado para o Amazon Inspector, ele habilita automaticamente o acesso confiável para o Amazon Inspector na sua organização.

No entanto, se você deseja configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, chame explicitamente a operação `EnableAWSServiceAccesse` forneça a entidade de serviço principal como um parâmetro. Você então poderá chamar `EnableDelegatedAdminAccount` para delegar a conta de administrador do Inspector.

Você pode habilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para habilitar o acesso confiável a serviços usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  É possível executar o comando a seguir para habilitar o Amazon Inspector como um serviço confiável com o Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

> **Note**
>
> Se estiver usando a API `EnableAWSServiceAccess`, você também precisará chamar `EnableDelegatedAdminAccount` para delegar a conta de administrador do Inspector.

### Para desabilitar o acesso confiável com o Amazon Inspector

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador na conta de gerenciamento do AWS Organizations pode desabilitar acesso confiável com o Amazon Inspector.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  É possível executar o comando a seguir para desabilitar o Amazon Inspector como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

## Habilitar uma conta de administrador delegado do Amazon Inspector

Com o Amazon Inspector, você pode gerenciar várias contas em uma organização usando um administrador delegado com o serviço AWS Organizations.

A conta de gerenciamento AWS Organizations designa uma conta na organização como conta do administrador delegado do Amazon Inspector. O administrador delegado gerencia o Amazon Inspector para a organização e recebe permissões especiais para executar tarefas em nome de sua organização, como: habilitar ou desabilitar verificações de contas-membro, exibir dados de localização agregados de toda a organização e criar e gerenciar regras de supressão

Para obter informações sobre como um administrador delegado gerencia contas da organização, consulte Compreender o relacionamento entre contas de administrador e membro no Guia do usuário do Amazon Inspector.

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para o Amazon Inspector.

É possível especificar uma conta de administrador delegado via console ou API do Amazon Inspector ou usando a operação da CLI ou do SDK do Organizations.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como administrador delegado do Amazon Inspector na organização

Para configurar um administrador delegado usando o console do Amazon Inspector, consulte Etapa 1: Habilitar o Amazon Inspector - Ambiente de várias contas no Guia do usuário do Amazon Inspector.

> **Note**
>
> Você deve ligar para `inspector2:enableDelegatedAdminAccount` em cada região em que você usa o Amazon Inspector.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, poderá usar os seguintes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK: chame a operação `RegisterDelegatedAdministrator` do Organizations e o número de ID da conta-membro e identifique a entidade principal do serviço de conta `account.amazonaws.com` como parâmetros.

### Desabilitar um administrador delegado do Amazon Inspector

Somente um administrador na conta de gerenciamento da AWS Organizations pode remover uma conta de administrador delegado da organização.

É possível remover a conta de administrador delegado via console ou API do Amazon Inspector ou usando a operação `DeregisterDelegatedAdministrator` da CLI ou o SDK do Organizations. Para remover um administrador delegado usando o console do Amazon Inspector, consulte Remover um administrador delegado no Guia do usuário do Amazon Inspector.

## AWS License Manager e AWS Organizations

O AWS License Manager simplifica o processo de transferir as licenças de fornecedor de software para a nuvem. À medida que você desenvolve a infraestrutura de nuvem no AWS, pode reduzir os custos usando as oportunidades de Bring-Your-Own-License (BYOL) ou seja, redirecionando seu inventário de licenças existente para uso com os recursos de nuvem. Com controles baseados em regras no consumo de licenças, os administradores podem definir limites rígidos ou flexíveis em implantações de nuvem novas e existentes, interrompendo o uso de servidor não compatível antes de acontecer.

Para obter mais informações sobre o License Manager, consulte o Guia do License Manager.

Ao vincular o License Manager ao AWS Organizations, é possível:

- Habilitar a descoberta entre contas de recursos de computação em toda a sua organização.

- Visualizar e gerenciar assinaturas comerciais do Linux que você possui e usa naAWS. Para obter mais informações, consulte Assinaturas Linux no AWS License Manager.

Use as informações a seguir para ajudá-lo a integrar o AWS License Manager ao AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

As funções vinculadas ao serviço a seguir são criadas automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essas funções permitem que o License Manager realize operações válidas nas contas de sua organização.

Você só poderá excluir ou modificar essas funções se desabilitar o acesso confiável entre o License Manager e o Organizations, ou se remover a conta-membro da organização.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

Para obter mais informações, consulte License Manager — Perfil de conta de gerenciamento, License Manager — Perfil de conta-membro e License Manager — Perfil de assinaturas Linux.

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo License Manager concedem acesso às seguintes entidades de serviço primárias:

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

## Habilitar o acesso confiável no License Manager

Você pode habilitar o acesso confiável usando apenas o AWS License Manager.

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Para habilitar o acesso confiável com o License Manager

Você deve fazer login no console do License Manager usando sua conta de gerenciamento do AWS Organizations e associá-la à sua conta do License Manager. Para obter mais informações, consulte Configurações no AWS License Manager.

## Desabilitar o acesso confiável no License Manager

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

É possível desabilitar o acesso confiável executando um comando da AWS CLI do Organizations ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS License Manager como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-manager.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

  Para desabilitar o acesso confiável para as assinaturas Linux, use:

  ```
  $  aws organizations disable-aws-service-access \
      --service-principal license-manager-linux-subscriptions.amazonaws.com
  ```

- AWS API: DisableAWSServiceAccess

### Habilitar uma conta de administrador delegado para o License Manager

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e funções dessa conta podem executar ações administrativas para o License Manager que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do License Manager.

Para delegar uma conta-membro como administrador para o License Manager, siga as etapas em Registrar um administrador delegado no Guia do usuário do License Manager.

## Amazon Macie e o AWS Organizations

O Amazon Macie é um serviço de segurança e privacidade de dados totalmente gerenciado que usa machine learning e comparação de padrões para detectar, monitorar e ajudar você a proteger seus dados confidenciais no Amazon Simple Storage Service (Amazon S3). O Macie automatiza a descoberta de dados sigilosos, como informações de identificação pessoal (PII) e propriedade intelectual, para fornecer uma melhor compreensão dos dados armazenados por sua organização no Amazon S3.

Para obter mais informações, consulte Gerenciar contas do Amazon Macie com o AWS Organizations no Guia do usuário do Amazon Macie.

Use as informações a seguir para ajudá-lo a integrar o Amazon Macie ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente para a conta de administrador delegado do Macie da sua organização quando você habilita o acesso confiável. Essa função permite que o Macie execute as operações suportadas nas contas da sua organização.

Você só pode excluir essa função se desabilitar o acesso confiável entre o Macie e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleRorAmazonMacie`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções

vinculadas ao serviço usadas pelo Macie concedem acesso às seguintes entidades de serviço primárias:

- `macie.amazonaws.com`

## Habilitar o acesso confiável no Macie

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do Amazon Macie ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do Amazon Macie para habilitar a integração com o Organizations. Isso permite que o Amazon Macie realize qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo Amazon Macie. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o console ou as ferramentas do Amazon Macie, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando o console do Macie

O Amazon Macie requer acesso confiável ao AWS Organizations para designar uma conta-membro como administrador do Macie para a sua organização. Se você configurar um administrador delegado usando o console de gerenciamento do Macie, o Macie habilita automaticamente o acesso confiável para você.

Para obter mais informações, consulteIntegrar e configurar uma organização no Amazon Macie no Guia do usuário do Amazon Macie.

Você pode habilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para habilitar o acesso confiável a serviços usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o Amazon Macie como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

## Habilitar uma conta de administrador delegado para o Macie

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e funções dessa conta podem executar ações administrativas para o Macie que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Macie.

**Permissões mínimas**

Somente um usuário ou perfil na conta de gerenciamento do Organizations com as seguintes permissões pode configurar uma conta-membro como administrador delegado para o Macie na organização:

- `organizations:EnableAWSServiceAccess`
- `macie:EnableOrganizationAdminAccount`

Para designar uma conta-membro como administrador delegado do Macie

O Amazon Macie requer acesso confiável ao AWS Organizations para designar uma conta-membro como administrador do Macie para a sua organização. Se você configurar um administrador delegado usando o console de gerenciamento do Macie, o Macie habilita automaticamente o acesso confiável para você.

Para obter mais informações, consulte https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin.

## AWS Marketplace e AWS Organizations

O AWS Marketplace é um catálogo digital selecionado que você pode usar de encontrar, comprar, implantar e gerenciar o software, os dados e os serviços de terceiros de que você precisa para desenvolver soluções e administrar sua empresa.

O AWS Marketplace cria e gerencia licenças usando o AWS License Manager para suas compras no AWS Marketplace. Quando você compartilha (concede acesso a) suas licenças com outras contas de sua organização, o AWS Marketplace cria e gerencia novas licenças para essas contas.

Para obter mais informações, consulte Funções vinculadas ao serviço para o AWS Marketplace no Guia do comprador do AWS Marketplace.

Use as informações a seguir para ajudá-lo a integrar o AWS Marketplace ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o AWS Marketplace realize as operações suportadas nas contas de sua organização.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o AWS Marketplace e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForMarketplaceLicenseManagement`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo AWS Marketplace concedem acesso às seguintes entidades de serviço primárias:

- `license-management.marketplace.amazonaws.com`

## Habilitar o acesso confiável no AWS Marketplace

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Marketplace ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Marketplace para habilitar a integração com o Organizations. Isso permite que o AWS Marketplace execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Marketplace. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Marketplace, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando o console do AWS Marketplace

Consulte Creating a service-linked role for AWS Marketplace (Criar um perfil vinculado ao serviço para o AWS Marketplace) no Guia do comprador do AWS Marketplace.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Marketplace, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).

3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Marketplace que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Marketplace como um serviço confiável com o Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no AWS Marketplace

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Marketplace como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

## AWS Marketplace Marketplace privado e AWS Organizations

AWS Marketplace é um catálogo digital com curadoria que você pode usar para encontrar, comprar, implantar e gerenciar software, dados e serviços de terceiros necessários para criar soluções e administrar seus negócios. Um mercado privado fornece um amplo catálogo de produtos disponíveis em AWS Marketplace, juntamente com um controle refinado desses produtos.

AWS Marketplace O Private Marketplace permite que você crie várias experiências de mercado privado associadas a toda a sua organização, a uma ou mais OUs ou a uma ou mais contas em sua organização, cada uma com seu próprio conjunto de produtos aprovados. Seus AWS administradores também podem aplicar a marca da empresa a cada experiência de mercado privado com o logotipo, as mensagens e o esquema de cores da sua empresa ou equipe.

Para obter mais informações, consulte Usando funções para configurar o Private Marketplace AWS Marketplaceno Guia doAWS Marketplace comprador.

Use as informações a seguir para ajudá-lo a integrar o AWS Marketplace Private Marketplace com AWS Organizationso.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento da sua organização quando você ativa o acesso confiável usando o console do Private AWS Marketplace Marketplace. Essa função permite que o Private Marketplace realize operações

suportadas nas contas de sua organização em sua organização. Você pode excluir ou modificar essa função somente se desativar o acesso confiável entre o AWS Marketplace Private Marketplace e o Organizations e desassociar todas as experiências de mercado privado em sua organização.

Se você habilitar o acesso confiável diretamente do console, CLI ou SDK do Organizations, a função vinculada ao serviço não será criada automaticamente.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Private Marketplace concedem acesso aos seguintes diretores de serviço:

- `private-marketplace.marketplace.amazonaws.com`

## Habilitando acesso confiável com o Private Marketplace

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Marketplace Private Marketplace ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o console ou as ferramentas do AWS Marketplace Private Marketplace para permitir a integração com o Organizations. Isso permite que o AWS Marketplace Private Marketplace execute qualquer configuração necessária, como criar os recursos necessários para o serviço. Continue com essas etapas somente se você não conseguir habilitar a integração usando as ferramentas fornecidas pelo AWS Marketplace Private Marketplace. Para obter mais informações, consulte esta nota. Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Marketplace Private Marketplace, não precisará concluir essas etapas.

Para habilitar o acesso confiável usando o console do Private Marketplace

Consulte Introdução ao Private Marketplace no Guia doAWS Marketplace comprador.

Você pode ativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando ou chamando uma operação de API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console doAWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Serviços, localize a linha do AWS Marketplace Private Marketplace, escolha o nome do serviço e escolha Habilitar acesso confiável.
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for administrador do Only AWS Organizations, diga ao administrador do AWS Marketplace Private Marketplace que agora ele pode habilitar esse serviço usando seu console para trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Marketplace Private Marketplace como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Ativar AWSServiceAccess

## Desativando o acesso confiável com o Private Marketplace

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desativar o acesso confiável executando um AWS CLI comando Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável a serviços:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desativar o AWS Marketplace Private Marketplace como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSServiceAccess

## Habilitando uma conta de administrador delegado para o Private Marketplace

O administrador da conta de gerenciamento pode delegar permissões administrativas do Private Marketplace a uma conta de membro designada conhecida como administrador delegado. Para registrar uma conta como administrador delegado no mercado privado, o administrador da conta de gerenciamento deve garantir que o acesso confiável e a função vinculada ao serviço estejam habilitados, escolher Registrar um novo administrador, fornecer o número da AWS conta de 12 dígitos e escolher Enviar.

Contas de gerenciamento e contas de administrador delegado podem realizar tarefas administrativas do Private Marketplace, como criar experiências, atualizar configurações de marca, associar ou desassociar públicos, adicionar ou remover produtos e aprovar ou recusar solicitações pendentes.

Para configurar um administrador delegado usando o console do Private Marketplace, consulte Criação e gerenciamento de um mercado privado no Guia doAWS Marketplace comprador.

Você também pode configurar um administrador delegado usando a `RegisterDelegatedAdministrator` API Organizations. Para obter mais informações, consulte RegisterDelegatedAdministratorna Referência de Comandos do Organizations.

### Desabilitando um administrador delegado para o Private Marketplace

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para o Private Marketplace.

Você pode remover o administrador delegado usando o console ou a API do Private Marketplace, ou usando a operação `DeregisterDelegatedAdministrator` CLI ou SDK do Organizations.

Para desativar a conta do administrador delegado do Private Marketplace usando o console do Private Marketplace, consulte Criação e gerenciamento de um mercado privado no Guia do AWS Marketplace comprador

## AWS Gerente de rede e AWS Organizations

O Network Manager permite que você gerencie centralmente sua rede principal AWS Cloud WAN e sua rede AWS Transit Gateway em todas as AWS contas, regiões e locais locais. Com o suporte para várias contas, você pode criar uma única rede global para qualquer uma de suas AWS contas e registrar gateways de trânsito de várias contas na rede global usando o console do Network Manager.

Com o acesso confiável habilitado entre o Network Manager e o Organizations, os administradores delegados registrados e as contas de gerenciamento podem utilizar a função vinculada ao serviço implantada nas contas membros para descrever os recursos anexados às suas redes globais.
No console do Network Manager, os administradores delegados registrados e as contas de gerenciamento podem assumir os perfis do IAM personalizados implantados nas contas de membro: `CloudWatch-CrossAccountSharingRole` para monitoramento e eventos em várias contas, e `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess` para o acesso à função de switch do console para visualizar e gerenciar recursos de várias contas)

> **Important**
>
> - É altamente recomendável usar o console do Network Manager para gerenciar configurações de várias contas (habilitar/desabilitar o acesso confiável e registrar/cancelar

o registro de administradores delegados). O gerenciamento dessas configurações no console implanta e gerencia automaticamente todas as funções vinculadas ao serviço necessárias e perfis do IAM personalizados para as contas de membros necessárias para o acesso a várias contas.

- Quando você ativa o acesso confiável para o Network Manager no console do Network Manager, o console também ativa o AWS CloudFormation StackSets serviço. O Network Manager usa StackSets para implantar as funções personalizadas do IAM necessárias para o gerenciamento de várias contas.

Para obter mais informações sobre como integrar o Network Manager ao Organizations, consulte Gerenciar várias contas no Network Manager com o  AWS Organizations no Guia do usuário da Amazon VPC.

Use as informações a seguir para ajudá-lo a integrar o AWS Network Manager com AWS Organizations o.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

Ao habilitar o acesso confiável, as seguintes funções vinculadas a serviços serão automaticamente criadas nas contas listadas da organização. Tais funções permitem que o Network Manager realize as operações compatíveis nas contas da sua organização. Se você desabilitar o acesso confiável, o Network Manager não excluirá tais perfis de contas na sua organização. Você pode excluí-los manualmente usando o console do IAM.

Conta de gerenciamento

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

Contas-membro

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Quando você registra uma conta de membro como um administrador delegado, a função adicional a seguir será criada automaticamente na conta de administrador delegado:

- `AWSServiceRoleForCloudWatchCrossAccount`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

As funções vinculadas a serviços só podem ser assumidas pelas entidades principais de serviço autorizadas pelas relações de confiança definidas para a função.

- Para a função `AWSServiceRoleForNetworkManager service-linked`, `networkmanager.amazonaws.com` é a única entidade principal de serviço com acesso.
- Para a função vinculada ao serviço `AWSServiceRoleForCloudFormationStackSetsOrgMember`, `member.org.stacksets.cloudformation.amazonaws.com` é a única entidade principal de serviço com acesso.
- Para a função vinculada ao serviço `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`, `stacksets.cloudformation.amazonaws.com` é a única entidade principal de serviço com acesso.
- Para a função vinculada ao serviço `AWSServiceRoleForCloudWatchCrossAccount`, `cloudwatch-crossaccount.amazonaws.com` é a única entidade principal de serviço com acesso.

A exclusão dessas funções prejudicará a funcionalidade de várias contas para o Network Manager.

## Como habilitar o acesso confiável com o Network Manager

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Somente um administrador na conta de gerenciamento do Organizations tem permissões para habilitar o acesso confiável a outro AWS serviço. Certifique-se de usar o console do Network Manager para habilitar o acesso confiável a fim de evitar problemas de permissões. Para obter mais informações, consulte Gerenciar várias contas no Network Manager com o  AWS Organizations no Guia do usuário da Amazon VPC.

### Como desabilitar o acesso confiável no Network Manager

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Somente um administrador em uma conta de gerenciamento do Organizations tem permissões para desativar o acesso confiável com outro AWS serviço.

> **Important**
>
> Recomendamos que você use o console do Network Manager para desabilitar o acesso confiável. Se você desabilitar o acesso confiável de qualquer outra forma, como usando AWS CLI, com uma API ou com o AWS CloudFormation console, as funções do IAM implantadas AWS CloudFormation StackSets e personalizadas podem não ser devidamente eliminadas. Para desabilitar o acesso confiável, faça login no console do Network Manager.

### Como habilitar uma conta de administrador delegado para o Network Manager

Quando você designa uma conta de membro como um administrador delegado para a organização, os usuários e as funções dessa conta podem executar ações administrativas para o Network Manager que, de outra forma, só poderiam ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Network Manager.

Para obter instruções sobre como designar uma conta de membro como administrador delegado do Network Manager na organização, consulte Registro de um administrador delegado no Guia do usuário da Amazon VPC.

## Desenvolvedor Amazon Q (Amazon Q) e AWS Organizations

O Amazon Q Developer é um assistente de conversação com inteligência artificial generativa (IA) que pode ajudar você a entender, criar, ampliar e operar AWS aplicativos. A versão de assinatura paga do Amazon Q requer integração com Organizations. Para obter mais informações, consulte Configuração de Account, IAM Identity Center e Organizations no guia do usuário do Amazon Q.

Use as informações a seguir para ajudá-lo a integrar o Amazon Q Developer com AWS Organizations o.

## Perfis vinculados ao serviço

A função `AWSServiceRoleForAmazonQDeveloper` vinculada ao serviço permite que a Amazon Q realize operações suportadas nas contas da sua organização em sua organização. Crie a função usando o console, a API ou a CLI do Amazon Q, conforme descrito em Criação de uma função vinculada ao serviço no Guia do usuário do IAM.

Você pode excluir ou modificar essa função somente se você desabilitar o acesso confiável entre Amazon Q e Organizations, ou se você remover a conta membro da organização.

## Princípios de serviço usados pela Amazon Q

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Amazon Q concedem acesso às seguintes entidades de serviço:

- `q.amazonaws.com`

## Habilitando o acesso confiável com o Amazon Q

O Amazon Q usa acesso confiável para compartilhar as configurações feitas no nível da organização com as contas dos membros. Por exemplo, o administrador no nível de Organizations pode ativar o Recurso X, e o Recurso X estará então disponível para todas as contas membros da mesma organização. Para obter mais informações, consulte Setting up Organizations no guia do usuário do Amazon Q Developer.

Você pode habilitar o acesso confiável usando somente o Amazon Q Developer.

Para ativar o acesso confiável para o Amazon Q, no console do Amazon Q, siga as instruções em Assinaturas no guia do usuário do Amazon Q Developer. Na Etapa 6, selecione Compartilhar perfil de configurações com contas de membros.

## Desabilitando o acesso confiável com o Amazon Q

Você pode desativar o acesso confiável usando somente as ferramentas Amazon Q Developer.

Para desativar o acesso confiável ao Amazon Q, no console do Amazon Q, siga as instruções em Assinaturas no guia do usuário do Amazon Q Developer. Na Etapa 6, desmarque Compartilhar perfil de configurações com contas de membros.

# AWS Resource Access Manager e AWS Organizations

O AWS Resource Access Manager (AWS RAM) permite compartilhar recursos especificados da AWS que você possui com outras Contas da AWS. Ele é um serviço centralizado que fornece uma experiência consistente para compartilhar diferentes tipos de recursos da AWS em várias contas.

Para obter mais informações sobre o AWS RAM, consulte o Guia do usuário do AWS RAM.

Use as informações a seguir para ajudá-lo a integrar o AWS Resource Access Manager ao AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o AWS RAM realize as operações suportadas nas contas de sua organização.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o AWS RAM e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForResourceAccessManager`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo AWS RAM concedem acesso às seguintes entidades de serviço primárias:

- `ram.amazonaws.com`

## Habilitar o acesso confiável no AWS RAM

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Resource Access Manager ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Resource Access Manager para habilitar a integração com o Organizations. Isso permite que o AWS Resource Access Manager execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Resource Access Manager. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Resource Access Manager, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando o console ou a CLI do AWS RAM

Consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Resource Access Manager, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Resource Access Manager que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Resource Access Manager como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no AWS RAM

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando as ferramentas do AWS Resource Access Manager ou do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Resource Access Manager para desabilitar a integração com o Organizations. Isso permite que o AWS Resource Access Manager realize qualquer limpeza necessária, como excluir recursos ou funções de acesso que não são mais necessários para o serviço. Continue com estas etapas apenas se você não puder desabilitar a integração usando as ferramentas fornecidas pelo AWS Resource Access Manager.
> Se você desabilitar o acesso confiável usando o console ou as ferramentas do AWS Resource Access Manager, não é necessário concluir estas etapas.

Desabilitar o acesso confiável usando o console ou a CLI do AWS Resource Access Manager

Consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS Resource Access Manager e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Resource Access Manager que agora ele pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Resource Access Manager como um serviço confiável com o Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ram.amazonaws.com
```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

## Explorador de recursos da AWS e AWS Organizations

O Explorador de recursos da AWS é um serviço de pesquisa e descoberta de recursos. Com o Explorador de Recursos, você pode descobrir seus recursos, como instâncias do Amazon Elastic Compute Cloud, o Amazon Kinesis Data Streams ou tabelas do Amazon DynamoDB, por meio de uma experiência semelhante ao uso de um mecanismo de busca na Internet. Você pode pesquisar seus recursos usando metadados de recursos, como nomes, tags e IDs. O Explorador de Recursos funciona em todas as regiões da AWS na sua conta para simplificar suas workloads entre regiões.

Ao integrar o Explorador de Recursos ao AWS Organizations, você pode coletar evidências de uma fonte mais ampla colocando várias Contas da AWS de sua organização dentro do escopo de suas avaliações.

Use as informações a seguir para ajudá-lo a integrar o Explorador de recursos da AWS ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Esse perfil permite que o Explorador de Recursos realize operações compatíveis nas contas da sua organização.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o Explorador de Recursos e o Organizations, ou se remover a conta-membro da organização.

Para obter mais informações sobre como o Explorador de Recursos utiliza esse perfil, consulte Using service-linked roles no Guia do usuário do Explorador de recursos da AWS.

- `AWSServiceRoleForResourceExplorer`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. Os perfis vinculados ao serviço utilizados pelo Explorador de Recursos concedem acesso às seguintes entidades principais de serviço:

- `resource-explorer-2.amazonaws.com`

### Para habilitar o acesso confiável no Explorador de recursos da AWS

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

O Explorador de Recursos requer acesso confiável ao AWS Organizations para que você possa designar uma conta-membro como administrador delegado de sua organização.

Você pode habilitar o acesso confiável usando o console do Explorador de Recursos ou o console do Organizations. É altamente recomendável, sempre que possível, que você use o console ou as ferramentas do Explorador de Recursos para habilitar a integração com o Organizations. Isso permite que o Explorador de recursos da AWS execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço.

Para habilitar o acesso confiável usando o console do Explorador de Recursos

Para obter instruções sobre como habilitar o acesso confiável, consulte Prerequisites to using Resource Explorer no Guia do usuário do Explorador de recursos da AWS.

> **Note**
>
> Se você configurar um administrador delegado usando o console do Explorador de recursos da AWS, o Explorador de recursos da AWS habilita automaticamente o acesso confiável para você.

Você pode habilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para habilitar o acesso confiável a serviços usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

Você pode executar o comando a seguir para habilitar o Explorador de recursos da AWS como um serviço confiável com o Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

## Para desabilitar o acesso confiável com o Explorador de Recursos

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador na conta de gerenciamento do AWS Organizations pode desabilitar acesso confiável com o Explorador de recursos da AWS.

Você pode desabilitar o acesso confiável usando as ferramentas do Explorador de recursos da AWS ou do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do Explorador de recursos da AWS para desabilitar a integração com o Organizations. Isso permite que o Explorador de recursos da AWS realize qualquer limpeza necessária, como excluir recursos ou funções de acesso que não são mais necessários para o serviço. Continue com estas etapas apenas se você não puder desabilitar a integração usando as ferramentas fornecidas pelo Explorador de recursos da AWS.
> Se você desabilitar o acesso confiável usando o console ou as ferramentas do Explorador de recursos da AWS, não é necessário concluir estas etapas.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o Explorador de recursos da AWS como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

## Como habilitar uma conta de administrador delegado para o Explorador de Recursos

Use sua conta de administrador delegado para criar visualizações de recursos de várias contas e direcioná-las para uma unidade organizacional ou para toda a organização. É possível compartilhar visualizações de várias contas com qualquer conta da sua organização por meio do AWS Resource Access Manager criando compartilhamentos de recursos.

> **Permissões mínimas**
>
> Apenas um usuário ou perfil na conta de gerenciamento do Organizations com a seguinte permissão pode configurar uma conta-membro como administrador delegado para o Explorador de Recursos na organização: `resource-explorer:RegisterAccount`

Para obter instruções sobre como habilitar uma conta de administrador delegado para o Explorador de Recursos, consulte Configuração no Guia do usuário do Explorador de recursos da AWS.

Se você configurar um administrador delegado usando o console do Explorador de recursos da AWS, em seguida o Explorador de Recursos habilitará automaticamente o acesso confiável a você.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, poderá usar os seguintes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: chame a operação `RegisterDelegatedAdministrator` do Organizations e o número de ID da conta-membro e identifique o serviço de conta `resource-explorer-2.amazonaws.com` como parâmetros.

### Como desabilitar um administrador delegado para o Explorador de Recursos

Somente um administrador na conta de gerenciamento do Organizations ou na conta de administrador delegado do Explorador de Recursos podem remover um administrador delegado para o Explorador de Recursos. Você pode desabilitar o acesso confiável por meio da operação do SDK ou da CLI `DeregisterDelegatedAdministrator` do Organizations.

## AWS Security Hub e AWS Organizations

AWS Security Hub fornece uma visão abrangente do seu estado de segurança AWS e ajuda você a verificar seu ambiente em relação aos padrões e às melhores práticas do setor de segurança.

O Security Hub coleta dados de segurança de todos os seus serviços Contas da AWS, dos AWS serviços que você usa e dos produtos de parceiros terceirizados compatíveis. Ele ajuda você a analisar suas tendências de segurança e a identificar os problemas de segurança de maior prioridade.

Ao usar o Security Hub e AWS Organizations em conjunto, você pode habilitar automaticamente o Security Hub para todas as suas contas, incluindo novas contas à medida que elas são adicionadas. Isso aumenta a cobertura para as verificações e as detecções do Security Hub, o que fornece uma imagem mais completa e exata do seu procedimento de segurança em geral.

Para obter mais informações sobre o Security Hub, consulte o Guia do usuário doAWS Security Hub.

Use as informações a seguir para ajudá-lo a se integrar AWS Security Hub com AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Security Hub realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o Security Hub e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForSecurityHub`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Security Hub concedem acesso às seguintes entidades de serviço primárias:

- `securityhub.amazonaws.com`

### Habilitar o acesso confiável no Security Hub

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Quando você designa um administrador delegado para o Security Hub, o Security Hub habilita automaticamente o acesso confiável para o Security Hub em sua organização.

### Habilitar uma conta de administrador delegado para o Security Hub

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e funções dessa conta podem executar ações administrativas para o Security Hub que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Security Hub.

Para obter mais informações, consulte Designar uma conta de administrador do Security Hub no Guia do usuário doAWS Security Hub .

Para designar uma conta-membro como administrador delegado do Security Hub

1. Faça login com a sua conta de gerenciamento do Organizations.
2. Execute um dos seguintes:
   - Se sua conta de gerenciamento não tiver o Security Hub habilitado, no console do Security Hub, escolha Go to Security Hub (Ir para o Security Hub).
   - Se sua conta de gerenciamento tiver o Security Hub ativado, no console do Security Hub, em Geral, escolha Configurações.
3. Em Delegated Administrator (Administrador delegado), insira o ID da conta.

## O Amazon S3 Storage Lens e o AWS Organizations

Ao dar ao Amazon S3 Storage Lens acesso confiável à sua organização, você permite que ele colete e agregue métricas em todas as áreas da Contas da AWS sua organização. O S3 Storage Lens faz isso acessando a lista de contas que pertencem à sua organização e coleta e analisa as métricas de armazenamento, uso e atividade de todas elas.

Para obter mais informações, consulte Usar as funções vinculadas a serviços para o Amazon S3 Storage Lens no Guia do usuário do Amazon S3 Storage Lens.

Use as informações a seguir para ajudá-lo a integrar o Amazon S3 Storage Lens com o. AWS Organizations

### Função vinculada ao serviço criada quando você habilita a integração

A seguinte função vinculada a serviço é criada automaticamente na conta de administrador encarregada da sua organização quando você habilita o acesso confiável e a configuração do Storage Lens foi aplicada à sua organização. Essa função permite que o Amazon S3 realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o Amazon S3 Storage Lens e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForS3StorageLens`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Amazon S3 Storage Lens concedem acesso às seguintes entidades primárias de serviço:

- `storage-lens.s3.amazonaws.com`

## Habilitar o acesso confiável no Amazon S3 Storage Lens

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do Amazon S3 Storage Lens ou o console do AWS Organizations .

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do Amazon S3 Storage Lens para habilitar a integração com o Organizations. Isso permite que o Amazon S3 Storage Lens realize qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo Amazon S3 Storage Lens. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o console ou as ferramentas do Amazon S3 Storage Lens, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando o console do Amazon S3

Consulte Habilitando o acesso confiável para o S3 Storage Lens no Guia do usuário do Amazon Simple Storage Service.

Você pode ativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando ou chamando uma operação de API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o Amazon S3 Storage Lens, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador do Only AWS Organizations, diga ao administrador do Amazon S3 Storage Lens que agora ele pode habilitar esse serviço usando seu console para trabalhar. AWS Organizations

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o Amazon S3 Storage Lens como um serviço confiável com o Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Ativar AWSServiceAccess

## Desativação do acesso confiável para o Amazon S3 Storage Lens

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Amazon S3 Storage Lens.

Você pode desativar o acesso confiável usando o console do Amazon S3, o AWS CLI ou qualquer um dos AWS SDKs.

Para desabilitar o acesso confiável usando o console do Amazon S3

Consulte Desabilitar o acesso confiável para o S3 Storage Lens no Guia do usuário do Amazon Simple Storage Service.

## Habilitar uma conta de administrador delegado para o Amazon S3 Storage Lens

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e funções dessa conta podem executar ações administrativas para o Amazon S3 Storage Lens que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Amazon S3 Storage Lens.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations com a seguinte permissão pode configurar uma conta-membro como administrador delegado para o Amazon S3 Storage Lens na organização:
> `organizations:RegisterDelegatedAdministrator`
> `organizations:DeregisterDelegatedAdministrator`

O Amazon S3 Storage Lens suporta um máximo de 5 contas de administrador delegado em sua organização.

Para designar uma conta-membro como administrador delegado do Amazon S3 Storage Lens

Você pode registrar um administrador delegado usando o console do Amazon S3, AWS CLI o ou qualquer um dos SDKs. AWS Para registrar uma conta membro como uma conta de administrador delegado para sua organização usando o console Amazon S3, consulte Registro de um administrador delegado para o S3 Storage Lens no Guia do usuário do Amazon Simple Storage Service.

Para cancelar o registro de um administrador delegado para o Amazon S3 Storage Lens

Você pode cancelar o registro de um administrador delegado usando o console Amazon S3, o AWS CLI ou qualquer um dos SDKs. AWS Para cancelar o registro de um administrador delegado usando o console Amazon S3, consulte Cancelamento do registro de um administrador delegado para o S3 Storage Lens no Guia do usuário do Amazon Simple Storage Service.

## Amazon Security Lake e  AWS Organizations

O Amazon Security Lake centraliza dados de segurança de fontes na nuvem, on-premises e personalizadas em um data lake armazenado em sua conta. Ao se integrar ao Organizations, você pode criar um data lake que coleta registros e eventos em suas contas. Para obter mais informações, consulte Gerenciar várias contas com o AWS Organizations no Guia do usuário do Amazon Security Lake.

Use as informações a seguir para ajudá-lo a integrar o Amazon Security Lake com AWS Organizations o.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Amazon Security Lake realize operações suportadas nas contas da sua organização em sua organização.

Você pode excluir ou modificar essa função somente se desativar o acesso confiável entre o Amazon Security Lake e o Organizations, ou se remover a conta membro da organização.

- `AWSServiceRoleForSecurityLake`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Amazon Security Lake concedem acesso às seguintes entidades de serviço:

- `securitylake.amazonaws.com`

## Habilitando o acesso confiável com o Amazon Security Lake

Quando o acesso confiável for habilitado no Security Lake, o Security Lake poderá reagir automaticamente às alterações na associação à organização. O administrador delegado pode ativar a coleta de AWS registros de serviços compatíveis em qualquer conta da organização. Para obter mais informações, consulte Função vinculada ao serviço para o Amazon Security Lake no Guia do usuário do Amazon Security Lake.

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode ativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando ou chamando uma operação de API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Serviços, localize a linha para o Amazon Security Lake, escolha o nome do serviço e, em seguida, escolha Habilitar acesso confiável.
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for administrador do Only AWS Organizations, diga ao administrador do Amazon Security Lake que agora ele pode habilitar esse serviço usando seu console para trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  É possível executar o comando a seguir para habilitar o Amazon Security Lake como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Ativar AWSServiceAccess

## Desabilitando o acesso confiável com o Amazon Security Lake

Somente um administrador na conta de gerenciamento da Organizations pode desativar o acesso confiável com o Amazon Security Lake.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desativar o acesso confiável usando o AWS Organizations console, executando um AWS CLI comando do Organizations ou chamando uma operação da API Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Serviços, localize a linha do Amazon Security Lake e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for administrador do Only AWS Organizations, diga ao administrador do Amazon Security Lake que agora ele pode desativar esse serviço usando o console ou as ferramentas para não trabalhar com ele AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável a serviços:

- AWS CLI: disable-aws-service-access

  É possível executar o comando a seguir para desabilitar o Amazon Security Lake como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: Desativar AWSServiceAccess

## Habilitando uma conta de administrador delegado para o Amazon Security Lake

O administrador delegado do Amazon Security Lake adiciona outras contas na organização como contas membros. O administrador delegado pode ativar o Amazon Security Lake e definir as configurações do Amazon Security Lake para as contas dos membros. O administrador delegado pode coletar registros em toda a organização em todas as AWS regiões em que o Amazon Security Lake está habilitado (independentemente do endpoint regional que você está usando atualmente).

Você também pode configurar o administrador delegado para adicionar automaticamente novas contas na organização como membros. O administrador delegado do Amazon Security Lake tem acesso aos registros e eventos nas contas dos membros associados. Assim, você pode configurar o Amazon Security Lake para coletar dados pertencentes às contas de membros associadas. Também é possível conceder aos assinantes permissão para consumir dados pertencentes às contas-membro associadas.

Para obter mais informações, consulte Gerenciar várias contas com o AWS Organizations no Guia do usuário do Amazon Security Lake.

> **Permissões mínimas**
>
> Somente um administrador na conta de gerenciamento da Organizations pode configurar uma conta de membro como administrador delegado do Amazon Security Lake na organização

Você pode especificar uma conta de administrador delegado usando o console do Amazon Security Lake, a ação de `CreateDatalakeDelegatedAdmin` API do Amazon Security Lake ou o comando da `create-datalake-delegated-admin` CLI. Como alternativa, você pode usar a operação `RegisterDelegatedAdministrator` da CLI ou SDK do Organizations. Para obter instruções sobre como habilitar uma conta de administrador delegado para o Amazon Security Lake, consulte Designação do administrador delegado do Security Lake e adição de contas de membros no guia do usuário do Amazon Security Lake.

AWS CLI, AWS API

Se quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos SDKs, você pode usar AWS os seguintes comandos:

- AWS CLI:

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

- AWS SDK: chame a `RegisterDelegatedAdministrator` operação da Organizations e o número de identificação da conta do membro e identifique o responsável pelo serviço da conta `account.amazonaws.com` como parâmetros.

## Desabilitando um administrador delegado para o Amazon Security Lake

Somente um administrador na conta de gerenciamento do Organizations ou na conta de administrador delegado do Amazon Security Lake pode remover uma conta de administrador delegado da organização.

Você pode remover a conta de administrador delegado usando a ação de `DeleteDatalakeDelegatedAdmin` API do Amazon Security Lake, o comando `delete-datalake-delegated-admin` CLI ou usando a operação `DeregisterDelegatedAdministrator` CLI ou SDK do Organizations. Para remover um

administrador delegado usando o Amazon Security Lake, consulte Removendo o administrador delegado do Amazon Security Lake no guia do usuário do Amazon Security Lake.

## AWS Service Catalog e AWS Organizations

O permite criar e gerenciar os catálogos de serviços de TI aprovados para uso na AWS.

A integração do Catálogo de Serviços com o AWS Organizations simplifica o compartilhamento de portfólios e a cópia de produtos em uma organização. Os administradores do Catálogo de Serviços podem fazer referência a uma organização existente no AWS Organizations ao compartilhar um portfólio e podem compartilhar o portfólio com qualquer unidade organizacional (OU) confiável na estrutura em árvore da organização. Isso elimina a necessidade de compartilhar IDs de portfólio e da conta e de que a conta que está recebendo faça referência manual ao ID do portfólio ao importá-lo. Os portfólios compartilhados por meio desse mecanismo são listados na conta compartilhada na visualização Portfólio importado do administrador no Service Catalog.

Para obter mais informações sobre o Catálogo de Serviços, consulte o Guia do administrador do Service Catalog.

Use as informações a seguir para ajudá-lo a integrar o AWS Service Catalog ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

O AWS Service Catalog não cria funções vinculadas ao serviço como parte da habilitação de acesso confiável.

### Entidades de serviço primárias usadas para conceder permissões

Para habilitar o acesso confiável, você deve especificar a seguinte entidade de serviço primária:

- `servicecatalog.amazonaws.com`

### Habilitando o acesso confiável com o Service Catalog

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Service Catalog ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Service Catalog para habilitar a integração com o Organizations. Isso permite que o AWS Service Catalog execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Service Catalog. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Service Catalog, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando a AWS ou o SDK do Service Catalog

Chame um dos seguintes comandos ou operações:

- AWS CLI: aws servicecatalog enable-aws-organizations-access
- AWS SDKs: AWSServiceCatalog::EnableAWSOrganizationsAccess

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Service Catalog, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Service Catalog que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Service Catalog como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

## Desabilitando o acesso confiável com o Service Catalog

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Se você desabilitar o acesso confiável usando o AWS Organizations enquanto usa o Service Catalog, ele não excluirá seus compartilhamentos atuais, mas impedirá que você crie outros compartilhamentos em toda a sua organização. Os compartilhamentos atuais não serão sincronizados com a estrutura da sua organização se ela for alterada depois que você chamar essa ação.

Você pode desabilitar o acesso confiável usando as ferramentas do AWS Service Catalog ou do AWS Organizations.

**Important**

É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Service Catalog para desabilitar a integração com o Organizations. Isso permite que o AWS Service Catalog realize qualquer limpeza necessária, como excluir recursos ou funções de acesso que não são mais necessários para o serviço. Continue com estas etapas apenas

se você não puder desabilitar a integração usando as ferramentas fornecidas pelo AWS Service Catalog.
Se você desabilitar o acesso confiável usando o console ou as ferramentas do AWS Service Catalog, não é necessário concluir estas etapas.

Para desabilitar o acesso confiável usando a AWS ou o SDK do Service Catalog

Chame um dos seguintes comandos ou operações:

- AWS CLI: aws servicecatalog disable-aws-organizations-access
- AWS SDKs: DisableAWSOrganizationsAccess

Você pode desabilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS Service Catalog e escolha o nome do serviço.
3. Escolha Desabilitar acesso confiável.
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Desabilitar acesso confiável.
5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Service Catalog que agora ele pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Service Catalog como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

## Service Quotas e AWS Organizations

O Service Quotas é um serviço da AWS que permite que você visualize e gerencie suas cotas em um local central. As cotas, também conhecidas como limites, são o valor máximo para seus recursos, ações e itens em sua Conta da AWS.

Quando o Service Quotas está associado ao AWS Organizations, você pode criar um modelo de solicitação de cota para solicitar automaticamente aumentos de cota quando as contas são criadas.

Para obter mais informações sobre as cotas de serviço, consulte o Guia do usuário do Service Quotas.

Use as informações a seguir para ajudá-lo a integrar o Service Quotas ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Service Quotas realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o Service Quotas e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForServiceQuotas`

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Service Quotas concedem acesso às seguintes entidades de serviço primárias:

- `servicequotas.amazonaws.com`

### Habilitar o acesso confiável no Service Quotas

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando apenas o Service Quotas.

É possível habilitar o acesso confiável usando o console, a AWS CLI ou o SDK do Service Quotas:

- Para habilitar o acesso confiável usando o console do Service Quotas

  Faça login com sua conta de gerenciamento do AWS Organizations e configure o modelo no console do Service Quotas. Para obter mais informações, consulte Usar o modelo de cotas de serviço no Guia do usuário do Service Quotas.
- Para habilitar o acesso confiável usando a AWS CLI ou o SDK do Service Quotas

  Chame o seguinte comando ou operação:

  - AWS CLI: aws service-quotas associate-service-quota-template
  - AWS SDKs: AssociateServiceQuotaTemplate

## AWS IAM Identity Center e AWS Organizations

O AWS IAM Identity Center fornece acesso de logon único para todas as suas Contas da AWS e aplicativos de nuvem. Ele se conecta com o Microsoft Active Directory através do AWS Directory Service para permitir que os usuários nesse diretório façam login em um portal de acesso da AWS personalizado usando seus nomes de usuário e senha do Active Directory existentes. Do portal de acesso da AWS, os usuários têm acesso a todos os aplicativos em nuvem e da Contas da AWS para os quais têm permissões.

Para obter mais informações sobre o IAM Identity Center, consulte o Guia do usuário do AWS IAM Identity Center.

Use as informações a seguir para ajudá-lo a integrar o AWS IAM Identity Center ao AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o IAM Identity Center realize as operações suportadas nas contas de sua organização.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o IAM Identity Center e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForSSO`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo IAM Identity Center concedem acesso às seguintes entidades de serviço primárias:

- `sso.amazonaws.com`

## Habilitar o acesso confiável no IAM Identity Center

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS IAM Identity Center ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS IAM Identity Center para habilitar a integração com o Organizations. Isso permite que o AWS IAM Identity Center execute qualquer configuração exigida, como a criação dos

recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS IAM Identity Center. Para obter mais informações, consulte esta nota.
Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS IAM Identity Center, não é necessário concluir estas etapas.

O IAM Identity Center requer acesso confiável com o AWS Organizations para funcionar. O acesso confiável é habilitado quando você configura o IAM Identity Center. Para obter mais informações, consulte Conceitos básicos - Etapa 1: habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS IAM Identity Center, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS IAM Identity Center que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS IAM Identity Center como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no IAM Identity Center

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

O IAM Identity Center requer acesso confiável com o AWS Organizations para operar. Se você desabilitar o acesso confiável com o AWS Organizations enquanto estiver usando o IAM Identity Center, ele deixará de funcionar porque não consegue acessar a organização. Os usuários não podem usar o IAM Identity Center para acessar contas. As funções criadas pelo IAM Identity Center se mantêm, mas o serviço do IAM Identity Center não pode acessá-las. As funções vinculadas ao serviço do IAM Identity Center permanecem. Se reabilitar o acesso confiável, o IAM Identity Center continuará a operar como antes, sem que seja necessário reconfigurar o serviço.

Se você remover uma conta de sua organização, o IAM Identity Center automaticamente limpará quaisquer metadados e recursos, como a função vinculada ao serviço dele. Uma conta independente removida de uma organização não funciona mais com o IAM Identity Center.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS IAM Identity Center e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS IAM Identity Center que agora ele pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS IAM Identity Center como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

## Como habilitar uma conta de administrador delegado para o IAM Identity Center

Quando você designa uma conta de membro como um administrador delegado para a organização, os usuários e as funções dessa conta podem executar ações administrativas para o IAM Identity

Center que, de outra forma, só poderiam ser acionadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do IAM Identity Center.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta de membro como um administrador delegado para o IAM Identity Center na organização.

Para obter instruções sobre como habilitar uma conta de administrador delegado para o IAM Identity Center, consulte Delegated administration (Administração delegada) no Guia do usuário do AWS IAM Identity Center.

## AWS Systems Manager e AWS Organizations

O AWS Systems Manager é uma coleção de recursos que permitem visibilidade e controle dos recursos da AWS. Os seguintes recursos do Systems Manager funcionam com o Organizations em todas as Contas da AWS em sua organização:

- O System Manager Explorer, é um painel de operações personalizável que fornece informações sobre os recursos da AWS. Você pode sincronizar os dados de operações de todas as Contas da AWS de sua organização usando o Organizations e o Systems Manager Explorer. Para obter mais informações, consulte Systems Manager Explorer no Guia do usuário do AWS Systems Manager.
- O Change Manager do Systems Manager é um framework de gerenciamento de alterações corporativas para solicitar, aprovar, implementar e emitir relatórios sobre alterações operacionais na configuração e na infraestrutura de suas aplicações. Para obter mais informações, consulte Change Manager do AWS Systems Manager no Guia do usuário do AWS Systems Manager.
- O Systems Manager OpsCenter fornece um local central no qual engenheiros de operações e profissionais de TI podem visualizar, investigar e solucionar itens de trabalho operacional (OpsItems) relacionados a recursos da AWS. Quando você usa o OpsCenter com o Organizations, ele é capaz de trabalhar com o OpsItems com base em uma conta de gerenciamento (seja uma conta de gerenciamento do Organizations ou uma conta de administrador delegado do Systems Manager) e uma outra conta durante uma única sessão. Após configurados, os usuários podem realizar os seguintes tipos de ações:
  - Criar, visualizar e atualizar o OpsItems em outra conta.

- Visualizar informações detalhadas sobre os recursos da AWS especificados no OpsItems em outra conta.
- Iniciar os runbooks do Systems Manager Automation para corrigir problemas com recursos da AWS em outra conta.

Para obter mais informações, consulte AWS Systems Manager OpsCenter no Guia do usuário do AWS Systems Manager.

Use as informações a seguir para ajudá-lo a integrar o AWS Systems Manager ao AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Systems Manager realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o Systems Manager e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Systems Manager concedem acesso às seguintes entidades de serviço primárias:

- `ssm.amazonaws.com`

## Habilitar o acesso confiável no Systems Manager

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Systems Manager, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Systems Manager que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Systems Manager como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no Systems Manager

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

O Systems Manager requer acesso confiável com o AWS Organizations para sincronizar dados de operações entre todas as Contas da AWS de sua organização. Se você desativar o acesso confiável, o Systems Manager não sincroniza os dados das operações e reporta um erro.

Você pode desabilitar o acesso confiável usando apenas as ferramentas do Organizations.

Você pode desabilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS Management Console

Para desabilitar o acesso confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha do AWS Systems Manager e escolha o nome do serviço.
3. Escolha Disable trusted access (Desabilitar acesso confiável).
4. Na caixa de diálogo de confirmação, insira **`disable`** e, em seguida, escolha Disable trusted access (Desabilitar acesso confiável).
5. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Systems Manager que agora ele pode desabilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

Você pode executar o comando a seguir para desabilitar o AWS Systems Manager como um serviço confiável com o Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ssm.amazonaws.com
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

## Habilitar uma conta de administrador delegado para o Systems Manager

Quando você designa uma conta-membro como administrador delegado para a organização, os usuários e funções dessa conta podem executar ações administrativas para o Systems Manager que, de outra forma, só podem ser executadas por usuários ou funções na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Systems Manager.

Se você usa o Change Manager em uma organização, você usa uma conta de administrador delegado. Esta é a Conta da AWS que foi designada como a conta para gerenciar modelos de alteração, solicitações de alteração, runbooks de alteração e fluxos de trabalho de aprovação no Change Manager. A conta delegada gerencia as atividades de alteração em toda a organização. Quando você configura sua organização para uso com o Change Manager, você especifica qual das suas contas desempenhará essa função. Não precisa ser conta de gerenciamento da organização. Não é necessário ter a conta de administrador delegado se você usar o Change Manager com apenas uma conta.

Para designar uma conta-membro como administrador delegado, consulte os seguintes tópicos no Guia do usuário do AWS Systems Manager:

- Para o Explorer e o OpsCenter, consulte Configurar um administrador delegado.
- Para o Change Manager, consulte Setting up an organization and delegated account for Change Manager (Configurar uma organização e uma conta delegada para o Change Manager).

# Políticas de tag e AWS Organizations

As políticas de tag são um tipo de política no AWS Organizations que pode ajudar você a padronizar tags em todos os recursos das contas de sua organização. Para obter mais informações sobre políticas de tag, consulte Políticas de tag.

Use as informações a seguir para ajudá-lo a integrar as políticas de tag com o AWS Organizations.

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

O Organizations interage com as tags anexadas aos seus recursos usando a entidade de serviço primária a seguir.

- `tagpolicies.tag.amazonaws.com`

## Habilitar o acesso confiável para políticas de tag

Você pode habilitar o acesso confiável habilitando políticas de tag na organização ou usando o console do AWS Organizations.

> **Important**
>
> É altamente recomendável habilitar o acesso confiável habilitando políticas de tags. Isso permite que o Organizations realize as tarefas de configuração necessárias.

Você pode habilitar o acesso confiável para políticas de tag habilitando o tipo de política de tag no console do AWS Organizations. Para mais informações, consulte Habilitação de um tipo de política.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.

2. Na página Services (Serviços), localize a linha para políticas de tag, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador de políticas de tag que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar as políticas de tag como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: EnableAWSServiceAccess

### Desabilitar o acesso confiável com políticas de tag

Você pode desabilitar o acesso confiável para políticas de tag desabilitando o tipo de política de tag no console do AWS Organizations. Para mais informações, consulte Desabilitar um tipo de política.

## AWS Trusted Advisor e AWS Organizations

O AWS Trusted Advisor inspeciona seu ambiente da AWS e faz recomendações quando existem oportunidades de poupar, melhorar a performance do sistema ou ajudar a corrigir falhas de segurança. Quando integrado com o Organizations, você pode receber os resultados das

verificações do Trusted Advisor para todas as contas de sua organização e baixar relatórios para ver os resumos de suas verificações e todos os recursos afetados.

Para obter mais informações, consulte Visualização organizacional para o AWS Trusted Advisor no Guia do usuário do AWS Support.

Use as informações a seguir para ajudá-lo a integrar o AWS Trusted Advisor ao AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o Trusted Advisor realize as operações suportadas nas contas de sua organização.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o Trusted Advisor e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForTrustedAdvisorReporting`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Trusted Advisor concedem acesso às seguintes entidades de serviço primárias:

- `reporting.trustedadvisor.amazonaws.com`

## Habilitar o acesso confiável no Trusted Advisor

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando apenas o AWS Trusted Advisor.

Para habilitar o acesso confiável usando o console do Trusted Advisor

Consulte Habilitar a visualização organizacional no Guia do usuário do AWS Support.

## Desabilitar o acesso confiável no Trusted Advisor

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Depois que esse recurso é desabilitado, o Trusted Advisor para de registrar informações de verificação de todas as outras contas de sua organização. Não é possível exibir ou baixar relatórios existentes nem criar novos relatórios.

Você pode desabilitar o acesso confiável usando as ferramentas do AWS Trusted Advisor ou do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Trusted Advisor para desabilitar a integração com o Organizations. Isso permite que o AWS Trusted Advisor realize qualquer limpeza necessária, como excluir recursos ou funções de acesso que não são mais necessários para o serviço. Continue com estas etapas apenas se você não puder desabilitar a integração usando as ferramentas fornecidas pelo AWS Trusted Advisor.
>
> Se você desabilitar o acesso confiável usando o console ou as ferramentas do AWS Trusted Advisor, não é necessário concluir estas etapas.

Para desabilitar o acesso confiável usando o console do Trusted Advisor

Consulte Desabilitar a visualização organizacional no Guia do usuário do AWS Support.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

Você pode executar o comando a seguir para desabilitar o AWS Trusted Advisor como um serviço confiável com o Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

## Como habilitar uma conta de administrador delegado para o Trusted Advisor

Quando você designa uma conta-membro como administrador delegado da organização, os usuários e as funções da conta designada podem gerenciar os metadados da Conta da AWS de outras contas-membro na organização. Se você não habilitar uma conta de administrador delegado, essas tarefas só poderão ser executadas pela conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento de detalhes da sua conta.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como um administrador delegado para o Trusted Advisor na organização

Para obter instruções sobre como ativar uma conta de administrador delegado para o Trusted Advisor, consulte Registrar administradores delegados no Guia do usuário do AWS Support.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou um dos AWS SDKs, poderá usar os seguintes comandos:

- AWS CLI:

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

- AWS SDK: chame a operação `RegisterDelegatedAdministrator` do Organizations e o número de ID da conta-membro e identifique a entidade principal do serviço de conta `account.amazonaws.com` como parâmetros.

### Desabilitar um administrador delegado para o Trusted Advisor

É possível remover a conta de administrador delegado usando o console do Trusted Advisor ou a operação `DeregisterDelegatedAdministrator` da CLI ou do SDK do Organizations. Para obter informações sobre como desativar a conta do administrador delegado do Trusted Advisor usando o console do Trusted Advisor, consulte Cancelar o registro de administradores delegados no Guia do usuário do AWS Support.

## AWS Well-Architected Tool e AWS Organizations

O AWS Well-Architected Tool ajuda você a documentar o estado de suas workloads e as compara com as práticas recomendadas arquitetônicas mais recentes da AWS.

O uso do AWS Well-Architected Tool com o Organizations permite que tanto o AWS Well-Architected Tool como clientes do Organizations simplifiquem o processo de compartilhamento de recursos do AWS Well-Architected Tool com outros membros de sua organização.

Para obter mais informações, consulte Sharing your AWS Well-Architected Tool resources (Compartilhar seus recursos da AWS Well-Architected Tool) no Guia do usuário do .

Use as informações a seguir para ajudá-lo a integrar o AWS Well-Architected Tool ao AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Essa função permite que o AWS WA Tool realize as operações suportadas nas contas de sua organização.

Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o AWS WA Tool e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForWellArchitected`

A política de perfil de serviço é `AWSWellArchitectedOrganizationsServiceRolePolicy`

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo AWS WA Tool concedem acesso às seguintes entidades de serviço primárias:

- `wellarchitected.amazonaws.com`

## Habilitar o acesso confiável no AWS WA Tool

Permite a atualização de AWS WA Tool para refletir mudanças hierárquicas em uma organização.

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o console do AWS Well-Architected Tool ou o console do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Well-Architected Tool para habilitar a integração com o Organizations. Isso permite que o AWS Well-Architected Tool execute qualquer configuração exigida, como a criação dos recursos necessários para o serviço. Continue com estas etapas apenas se você não puder habilitar a integração usando as ferramentas fornecidas pelo AWS Well-Architected Tool. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Well-Architected Tool, não é necessário concluir estas etapas.

Para habilitar o acesso confiável usando o console do AWS WA Tool

Consulte Sharing your AWS Well-Architected Tool resources (Compartilhar seus recursos do AWS Well-Architected Tool) no Guia do usuário do AWS Well-Architected Tool.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Services (Serviços), localize a linha para o AWS Well-Architected Tool, escolha o nome do serviço e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for o administrador apenas do AWS Organizations, informe ao administrador do AWS Well-Architected Tool que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Você pode executar o comando a seguir para habilitar o AWS Well-Architected Tool como um serviço confiável com o Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável no AWS WA Tool

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você pode desabilitar o acesso confiável usando as ferramentas do AWS Well-Architected Tool ou do AWS Organizations.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do console ou das ferramentas do AWS Well-Architected Tool para desabilitar a integração com o Organizations. Isso permite que o AWS Well-Architected Tool realize qualquer limpeza necessária, como excluir recursos ou funções de acesso que não são mais necessários para o serviço. Continue com estas etapas apenas se você não puder desabilitar a integração usando as ferramentas fornecidas pelo AWS Well-Architected Tool.
>
> Se você desabilitar o acesso confiável usando o console ou as ferramentas do AWS Well-Architected Tool, não é necessário concluir estas etapas.

Para desabilitar o acesso confiável usando o console do AWS WA Tool

Consulte Sharing your AWS Well-Architected Tool resources (Compartilhar seus recursos do AWS Well-Architected Tool) no Guia do usuário do AWS Well-Architected Tool.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Você pode executar o comando a seguir para desabilitar o AWS Well-Architected Tool como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: DisableAWSServiceAccess

# IP Address Manager (IPAM) da Amazon VPC e AWS Organizations

O IP Address Manager da Amazon VPC (IPAM) é um recurso da VPC que facilita o planejamento, o rastreamento e o monitoramento de endereços IP de suas workloads da AWS.

O uso do AWS Organizations permite monitorar o uso de endereços IP em toda a organização e compartilhar grupos de endereços IP entre contas-membro.

Para obter mais informações, consulte Integrar o IPAM ao AWS Organizations no Guia do usuário do IPAM da Amazon VPC.

Use as informações a seguir para ajudá-lo a integrar o IP Address Manager (IPAM) da Amazon VPC ao AWS Organizations.

## Funções vinculadas ao serviço, criadas quando você habilitou a integração

A seguinte função vinculada ao serviço é criada automaticamente na conta de gerenciamento da sua organização e em cada conta-membro quando você integra o IPAM ao AWS Organizations usando o console do IPAM ou usando a API `EnableIpamOrganizationAdminAccount` do IPAM.

- `AWSServiceRoleForIPAM`

Para obter mais informações, consulte Funções vinculadas ao serviço para IPAM no Guia do usuário do IPAM da Amazon VPC.

## Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo IPAM concedem acesso às seguintes entidades principais de serviço:

- `ipam.amazonaws.com`

## Para habilitar o acesso confiável no IPAM

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

> **Note**
>
> Quando você designa um administrador delegado para o IPAM, ele habilita automaticamente o acesso confiável para IPAM na sua organização.
> O IPAM requer acesso confiável ao AWS Organizations para que você possa designar uma conta-membro como administrador delegado desse serviço na sua organização.

É possível habilitar o acesso confiável usando apenas ferramentas do IP Address Manager (IPAM) da Amazon VPC.

Se você integrar o IPAM ao AWS Organizations usando o console ou a API `EnableIpamOrganizationAdminAccount` do IPAM, concederá automaticamente acesso confiável ao IPAM. Conceder acesso confiável cria a função vinculada ao serviço `AWSServiceRoleForIPAM` na conta de gerenciamento e em todas as contas-membro da organização. O IPAM usa a função vinculada ao serviço para monitorar CIDRs associados aos recursos de rede do EC2 em sua organização e para armazenar métricas relacionadas ao IPAM no Amazon CloudWatch. Para obter mais informações, consulte Funções vinculadas ao serviço para IPAM no Guia do usuário do IPAM da Amazon VPC.

Para obter instruções sobre como habilitar o acesso confiável, consulte Integrar o IPAM ao AWS Organizations no Guia do usuário do IPAM da Amazon VPC.

> **Note**
>
> Você não pode habilitar o acesso confiável com o IPAM usando o console do AWS Organizations ou com a API `EnableAWSServiceAccess`.

## Para desabilitar o acesso confiável com o IPAM

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Apenas um administrador na conta de gerenciamento do AWS Organizations pode desabilitar o acesso confiável no IPAM usando a API `disable-aws-service-access` do AWS Organizations.

Para obter informações sobre como desabilitar permissões de conta do IPAM e excluir a função vinculada ao serviço, consulte Funções vinculadas ao serviço para IPAM no Guia do usuário do IPAM da Amazon VPC.

Você pode desabilitar o acesso confiável executando um comando da AWS CLI do Organizations, ou chamando uma operação da API do Organizations em um dos AWS SDKs.

AWS CLI, AWS API

Para desabilitar o acesso confiável usando a CLI/SKD do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  É possível pode executar o comando a seguir para desabilitar o IP Address Manager (IPAM) da Amazon VPC como um serviço confiável no Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: DisableAWSServiceAccess

## Habilitar uma conta de administrador delegado do IPAM

A conta de administrador delegado do IPAM é responsável por criar o IPAM e os grupos de endereços IP, gerenciar e monitorar o uso de endereços IP na organização e compartilhar grupos de endereços IP entre contas-membro. Para obter mais informações, consulte Integrar o IPAM ao AWS Organizations no Guia do usuário do IPAM da Amazon VPC.

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado do IPAM.

É possível especificar uma conta de administrador delegado a partir do console do IPAM ou usando a API `enable-ipam-organization-admin-account`. Para obter mais informações, consulte enable-ipam-organization-admin-account na Referência de comandos da AWS AWS CLI.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como administrador delegado do IPAM na organização

Para configurar um administrador delegado usando o console do IPAM, consulte Integrar o IPAM ao AWS Organizations no Guia do usuário do IPAM da Amazon VPC.

### Desabilitar um administrador delegado do IPAM

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado do IPAM.

Para remover um administrador delegado usando a AWS AWS CLI, consulte disable-ipam-organization-admin-account na Referência de comandos da AWS AWS CLI.

Para desabilitar uma conta de administrador delegado usando o console do IPAM, consulte Integrar o IPAM ao AWS Organizations no Guia do usuário do IPAM da Amazon VPC.

## Amazon VPC Reachability Analyzer e AWS Organizations

O Reachability Analyzer é uma ferramenta de análise de configuração que possibilita a realização de testes de conectividade entre um recurso de origem e um recurso de destino em suas nuvens privadas virtuais (VPCs).

O uso do AWS Organizations com o Reachability Analyzer permite que você monitore caminhos entre contas em suas organizações.

Para obter mais informações, consulte Cross-account analyses for Reachability Analyzer (Análise entre contas para o Reachability Analyzer) no Guia do usuário do Reachability Analyzer.

Use as informações a seguir para ajudar você a integrar o Reachability Analyzer com o AWS Organizations.

### Funções vinculadas ao serviço, criadas quando você habilitou a integração

A função vinculada ao serviço a seguir é criada automaticamente na conta de gerenciamento de sua organização quando você habilita o acesso confiável. Esse perfil permite que o Reachability Analyzer execute operações com suporte nas contas da sua organização.

Só será possível excluir ou modificar essa função se você desabilitar o acesso confiável entre o Reachability Analyzer e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForReachabilityAnalyzer`

Para obter mais informações, consulte Cross-account analyses for Reachability Analyzer (Análise entre contas para o Reachability Analyzer) no Guia do usuário do Reachability Analyzer.

### Entidades de serviço primárias usadas pelas funções vinculadas ao serviço

A função vinculada ao serviço na seção anterior pode ser assumida apenas pelas entidades de serviço primárias autorizadas pelas relações de confiança definidas para a função. Os perfis vinculados ao serviço usados pelo Reachability Analyzer concedem acesso às entidades principais de serviço a seguir:

- `reachabilityanalyzer.networkinsights.amazonaws.com`

### Habilitar o acesso confiável com o Reachability Analyzer

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Quando você designa um administrador delegado para o Reachability Analyzer, o acesso confiável para o Reachability Analyzer é habilitado automaticamente na organização.

O Reachability Analyzer requer acesso confiável ao AWS Organizations para que você possa designar uma conta-membro como o administrador delegado desse serviço para sua organização.

> **Important**
>
> - É possível habilitar o acesso confiável usando o console do Reachability Analyzer ou o console do Organizations. No entanto, recomendamos fortemente o uso do console do Reachability Analyzer ou da API `EnableMultiAccountAnalysisForAwsOrganization` para habilitar a integração com o Organizations. Isso permite que o Reachability Analyzer execute qualquer configuração necessária, como a criação de recursos necessários para o serviço.
> - Conceder acesso confiável cria a função vinculada ao serviço `AWSServiceRoleForReachabilityAnalyzer` na conta de gerenciamento e em todas

as contas-membro da organização. O Reachability Analyzer usa o perfil vinculado ao serviço para permitir o gerenciamento, e o administrador delegado para executar análises de conectividade entre quaisquer recursos na organização. O Reachability Analyzer pode tirar snapshots dos elementos de rede das contas em uma organização para responder a consultas de conectividade.

- Para obter mais informações e instruções sobre como habilitar o acesso confiável por meio do Reachability Analyzer, consulte Cross-account analyses for Reachability Analyzer (Análise entre contas para o Reachability Analyzer) no Guia do usuário do Reachability Analyzer.

Você pode habilitar o acesso confiável usando o console do AWS Organizations, executando um comando da AWS CLI ou chamando uma operação da API em um dos AWS SDKs.

AWS Management Console

Para habilitar o acesso ao serviço confiável usando o console do Organizations

1. Faça login no console do AWS Organizations. Você deve fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário-raiz (não recomendado) na conta de gerenciamento da organização.
2. Na página Serviços, localize a linha para o VPC Reachability Analyzer, escolha o nome do serviço e, em seguida, selecione Habilitar acesso confiável.
3. Na caixa de diálogo de confirmação, habilite Show the option to enable trusted access (Mostrar a opção para habilitar acesso confiável), insira **`enable`** na caixa e, em seguida, escolha Enable trusted access (Habilitar acesso confiável).
4. Se você for administrador somente do AWS Organizations, informe ao administrador do Reachability Analyzer que agora ele pode habilitar esse serviço usando seu console para trabalhar com o AWS Organizations.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Você pode usar os comandos da AWS CLI ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

É possível executar o comando a seguir para habilitar o Reachability Analyzer como um serviço confiável com o Organizations.

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

Esse comando não gera nenhuma saída quando é bem-sucedido.

- AWS API: EnableAWSServiceAccess

## Desabilitar o acesso confiável com o Reachability Analyzer

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

É possível desabilitar o acesso confiável usando o console do Reachability Analyzer (recomendado) ou o console do Organizations. Para desabilitar o acesso confiável usando o console do Reachability Analyzer, consulte Cross-account analyses for Reachability Analyzer (Análise entre contas para o Reachability Analyzer) no Guia do usuário do Reachability Analyzer.

## Habilitar uma conta de administrador delegado para o Reachability Analyzer

A conta do administrador delegado pode executar análises de conectividade em qualquer um dos recursos da organização. Para obter mais informações, consulte Integrar o Reachability Analyzer ao AWS Organizations no Guia do usuário do Reachability Analyzer.

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para o Reachability Analyzer.

É possível especificar uma conta do administrador delegado usando o console do Reachability Analyzer ou a API `RegisterDelegatedAdministrator`. Para obter mais informações, consulte RegisterDelegatedAdministrator em Organizations Command Reference (Referência de comandos do Organizations).

> **Permissões mínimas**
>
> Somente um perfil ou usuário na conta de gerenciamento do Organizations pode configurar uma conta-membro como um administrador delegado para o Reachability Analyzer na organização

Para configurar um administrador delegado usando o console do Reachability Analyzer, consulte Integrar o Reachability Analyzer ao AWS Organizations no Guia do usuário do Reachability Analyzer.

### Desabilitar um administrador delegado para o Reachability Analyzer

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para o Reachability Analyzer.

É possível remover o administrador delegado usando o console ou a API do Reachability Analyzer ou usando a operação `DeregisterDelegatedAdministrator` da CLI ou do SDK do Organizations.

Para desabilitar a conta do administrador delegado do Reachability Analyzer usando o console do Reachability Analyzer, consulte Cross-account analyses for Reachability Analyzer (Análise entre contas para o Reachability Analyzer) no Guia do usuário do Reachability Analyzer.

## Administrador delegado para serviços da AWS que funcionam com o Organizations

Recomendamos usar a conta de gerenciamento do AWS Organizations e seus usuários e perfis somente para as tarefas que só podem ser executadas por essa conta. Também recomendamos armazenar todos os seus recursos da AWS em outras contas-membro na organização e mantê-las fora da conta de gerenciamento. Isso porque os recursos de segurança, como as políticas de controle de serviços (SCPs) do Organizations, não restringem usuários ou perfis na conta de gerenciamento. Separar seus recursos da sua conta de gerenciamento também pode ajudar a entender os lançamentos em suas faturas.

Muitos serviços da AWS que se integram ao Organizations permitem reduzir o uso da conta de gerenciamento. Esses serviços permitem que você registre uma ou mais contas-membro como administradores que podem gerenciar todas as contas da organização usadas no serviço. Essas contas são chamadas de administradores delegados para esse serviço específico. Ao registrar uma conta-membro como administrador delegado de um serviço da AWS, você permite que essa conta tenha algumas permissões administrativas para esse serviço, bem como permissões para ações somente leitura do Organizations.

Antes de registrar uma conta como administrador delegado de um serviço:

- Confirme se o serviço é compatível com administradores delegados. Consulte a tabela em AWS serviços que você pode usar com AWS Organizations para saber quais serviços oferecem suporte aos administradores delegados.

- Habilite o acesso confiável para o serviço em questão.

> **Note**
>
> Para saber como habilitar um administrador delegado para um serviço, consulte a tabela em AWS serviços que você pode usar com AWS Organizations e selecione o link Saiba mais na coluna Compatível com administrador delegado para esse serviço.

## Permissões concedidas a contas de administrador delegado

Cada conta de administrador delegado específica do serviço recebe permissões concedidas por esse serviço. Para saber mais, consulte a tabela em AWS serviços que você pode usar com AWS Organizations e selecione o link Saiba mais na coluna Compatível com administrador delegado para esse serviço.

Uma conta de administrador delegado também tem as seguintes permissões somente leitura:

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`

- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`

Essas permissões permitem a você visualizar, mas não alterar, esses itens do console:

- Estrutura da organização, todas as contas e OUs e políticas organizacionais
- Associações
- Todas as contas e OUs.
- Políticas organizacionais

# Segurança em AWS Organizations

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

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS Organizations, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Organizations. Os tópicos a seguir mostram como configurar o Organizations para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger os recursos de sua Organização.

Tópicos



## AWS PrivateLink para AWS Organizations

Com o AWS PrivateLink for AWS Organizations, você pode acessar o AWS Organizations serviço de dentro da Virtual Private Cloud (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 informações sobre como criar suas próprias VPCs, consulte o Guia do usuário da Amazon VPC.

Para conectar sua Amazon VPC a AWS Organizations, você deve primeiro definir uma interface VPC endpoint (endpoints de interface). Os endpoints de interface são representados por uma ou mais interfaces de rede elástica (ENIs) que recebem endereços IP privados de sub-redes em sua VPC. As solicitações de sua VPC para AWS Organizations mais de endpoints de interface permanecem na rede Amazon.

Para obter informações gerais sobre endpoints de interface, consulte Acessar um AWS serviço usando um endpoint VPC de interface no Guia do usuário da Amazon VPC.

Tópicos



## Limitações e restrições de AWS PrivateLink para AWS Organizations

As limitações da VPC se aplicam a AWS PrivateLink for. AWS Organizations Para obter mais informações, consulte Acessar um AWS serviço usando uma interface VPC endpoint e AWS PrivateLink cotas no Guia do usuário da Amazon VPC. Além disso, aplicam-se as seguintes restrições:

- Disponível somente na `us-east-1` região
- Não suporta Transport Layer Security (TLS) 1.1

## Criar um endpoint da VPC

Você pode criar um AWS Organizations endpoint em sua VPC usando o console Amazon VPC, AWS Command Line Interface o () ou.AWS CLI AWS CloudFormation

Para obter informações sobre como criar e configurar um endpoint usando o console da Amazon VPC ou o AWS CLI, consulte Criar um endpoint de VPC no Guia do usuário da Amazon VPC. Para

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

Ao criar um AWS Organizations endpoint, use o seguinte como nome do serviço:

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

Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS, use o seguinte nome de serviço FIPS: AWS Organizations

```
com.amazonaws.us-east-1.organizations-fips
```

## Criando uma política de endpoint da VPC para o AWS Organizations

Você pode anexar uma política de endpoint ao seu VPC endpoint que controla o acesso às Organizations. Essa política especifica as seguintes informações:

- A entidade principal que pode executar ações.
- As ações que podem ser executadas.
- Os recursos sobre os quais as ações podem ser realizadas.

Para obter mais informações, consulte Controle o acesso aos endpoints da VPC usando políticas de endpoint no Guia do usuário da Amazon VPC.

### Exemplo: política de endpoint da VPC para ações do AWS Organizations

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

# AWS Identity and Access Management e AWS Organizations

O acesso ao AWS Organizations requer credenciais. Essas credenciais devem ter permissões para acessar recursos do AWS, como um bucket do Amazon Simple Storage Service (Amazon S3), uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou uma unidade organizacional (UO) do AWS Organizations. As seções a seguir fornecem detalhes sobre como você pode usar o AWS Identity and Access Management (IAM) para ajudar a proteger o acesso à sua organização e controlar quem pode administrá-la.

Para determinar quem pode administrar quais partes de sua organização, o AWS Organizations usa o mesmo modelo de permissões baseadas no IAM que outros serviços da AWS. Como administrador na conta de gerenciamento de uma organização, você pode conceder permissões baseadas no IAM para executar tarefas do AWS Organizations anexando políticas a usuários, grupos e funções na conta de gerenciamento. Essas políticas especificam as ações que os principais podem executar. Você anexa uma política de permissões do IAM a um grupo do qual o usuário é membro ou diretamente a um usuário ou uma função. Como melhores práticas, recomendamos que você anexe políticas a grupos em vez de usuários. Você também pode conceder permissões de administrador completas a outros usuários.

Para a maioria das operações de administração do AWS Organizations, você precisa anexar permissões a usuários ou grupos na conta de gerenciamento. Se um usuário de uma conta-membro precisar realizar operações administrativas para a sua organização, você terá de conceder as permissões do AWS Organizations a uma função do IAM na conta de gerenciamento e habilitar o usuário da conta-membro para assumir a função. Para obter informações gerais sobre as políticas de permissões do &IAM consulte Visão geral de políticas do IAM no Manual do usuário do IAM.

Tópicos



## Autenticação

Você pode acessar a AWS usando qualquer um dos seguintes tipos de identidade:

- Usuário raiz da Conta da AWS – Quando se cadastra na AWS, você fornece um endereço de e-mail e uma senha que são associados à sua Conta da AWS. Estas são suas credenciais raiz e elas fornecem acesso total a todos os seus recursos da AWS.

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

- Usuário do IAM – Um usuário do IAM é simplesmente uma identidade na qual sua Conta da AWS tem permissões personalizadas específicas (por exemplo, para criar um sistema de arquivos no Amazon Elastic File System). Você pode usar uma senha e um nome de usuário do IAM para fazer login em páginas da Web seguras da AWS como AWS Management Console, Fóruns de discussão da AWS ou a Central de Suporte da AWS.

  Além de um nome e uma senha de usuário, você pode gerar chaves de acesso para cada usuário. Você pode usar essas chaves ao acessar serviços da AWS de forma programática, seja com um dos vários SDKs ou usando o AWS Command Line Interface (AWS CLI). As ferramentas de SDK e de AWS CLI usam as chaves de acesso para o cadastramento criptográfico da sua solicitação. Se você não usar essas ferramentas AWS, é necessário assinar a solicitação por conta própria. AWS Organizations oferece suporte a Signature Version 4, um protocolo para autenticação de solicitações de entrada da API. Para obter mais informações sobre solicitações de autenticação, consulte Solicitações de AWSAPI de assinatura no Guia do usuário do IAM.

- Função do IAM – Uma função do IAM é outra identidade do IAM que você pode criar em sua conta que tem permissões específicas. É semelhante a um usuário do &IAM mas não está associada a uma pessoa específica. Uma função do IAM permite obter chaves de acesso temporárias que podem acessar os serviços e recursos da AWS. Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

  - Acesso de usuário federado – Em vez de criar um usuário do IAM, você pode usar identidades de usuários já existentes do AWS Directory Service, o diretório de usuário de sua empresa ou um provedor de identidades da Web. Eles são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidades. Para obter mais informações sobre usuários federados, consulte Usuários federados e perfis no Guia do usuário do IAM.

- Acesso entre contas – Você pode usar uma função do IAM em sua conta para conceder, a outra Conta da AWS, permissões de acesso aos recursos de sua conta. Para ver um exemplo, consulte Tutorial: Delegar acesso entre Contas da AWS usando perfis do IAM no Manual do usuário do IAM.
- Acesso de serviço da AWS – É possível usar uma função do IAM em sua conta para conceder a um serviço da AWS permissões para acessar os recursos de sua conta. Por exemplo, é possível criar uma função que permita ao Amazon Redshift acessar um bucket do Amazon S3 em seu nome e carregar dados armazenados no bucket em um cluster do Amazon Redshift. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS serviço no Guia do usuário do IAM.
- Aplicativos executados no Amazon EC2 – Em vez de armazenar chaves de acesso na instância do EC2 para serem usadas pelos aplicativos em execução na instância e fazer solicitações de API da AWS, você pode usar uma função do IAM para gerenciar credenciais temporárias para esses aplicativos. Para atribuir uma função de AWS a uma instância de EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado à instância. Um perfil de instância contém a função e permite que programas em execução na instância EC2 obtenham credenciais temporárias. Para obter mais informações, consulte Uso de um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

## Controle de acesso

Você pode ter credenciais válidas para autenticar suas solicitações, mas, a menos que tenha permissões, não poderá administrar nem acessar recursos do AWS Organizations. Por exemplo, você deve ter permissões para criar uma UO ou para anexar uma política de controle de serviço (SCP) a uma conta.

As seções a seguir descrevem como gerenciar permissões para o AWS Organizations.

- Gerenciar permissões de acesso para a organização da AWS
- Uso de políticas baseadas em identidade (políticas do IAM) para o AWS Organizations
- Controle de acesso baseado em atributo com tags e AWS Organizations

# Gerenciar permissões de acesso para a organização da AWS

Todos os recursos da AWS, incluindo raízes, unidades organizacionais, contas e políticas de uma organização, pertencem a uma Conta da AWS, e permissões para criar ou acessar um recurso são controladas por políticas de permissão. No caso de uma organização, a conta de gerenciamento possui todos os recursos. Um administrador de contas pode controlar o acesso aos recursos da AWS ao anexar políticas de permissões a identidades do IAM (usuários, grupos e funções).

> **Note**
>
> O administrador de uma conta (ou o usuário administrador) é um usuário com permissões de administrador. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Ao conceder permissões, você decide quem recebe as permissões, para quais recursos as permissões são concedidas e as ações específicas que você deseja permitir nesses recursos.

Por padrão, usuários, grupos e funções do IAM não têm permissões. Como um administrador da conta de gerenciamento de uma organização, você pode executar tarefas administrativas ou delegar permissões de administrador a outros usuários ou funções do IAM na conta de gerenciamento. Para fazer isso, você anexa uma política de permissões do IAM a um usuário, grupo ou função do IAM. Por padrão, um usuário não tem permissões; isso é às vezes chamado de uma negação implícita. A política substitui a negação implícita com uma permissão explícita que especifica quais ações o usuário pode executar e em quais recursos eles podem executar as ações. Se as permissões forem concedidas a uma função, essa função poderá ser assumida por usuários em outras contas na organização.

## Recursos e operações do AWS Organizations

Esta seção aborda como os conceitos do AWS Organizations são mapeados para os conceitos equivalentes do IAM.

Recursos

No AWS Organizations, é possível controlar o acesso aos seguintes recursos:

- O raiz e as UOs que compõem a estrutura hierárquica de uma organização
- As contas que são membros da organização.

- As políticas que você anexa às entidades da organização
- Os handshakes que você usa para alterar o estado da organização

Cada um desses recursos tem um nome de recurso da Amazon (ARN) exclusivo associado a ele. Você controla o acesso a um recurso especificando seu Nome de região da Amazon (ARN) no elemento `Resource` de uma política de permissão do IAM. Para obter uma lista completa dos formatos de ARN para recursos usados emAWS Organizations, consulte Tipos de recursos definidos por AWS Organizations na Referência de Autorização de Serviço.

Operações

A AWS fornece um conjunto de operações para trabalhar com os recursos de uma organização. Eles permitem executar tarefas, como criar, listar, modificar, acessar o conteúdo e excluir recursos. A maioria das operações pode ser referenciada no elemento `Action` de uma política do IAM para controlar quem pode usar essa operação. Para ver uma lista de AWS Organizations operações que podem ser usadas como permissões em uma política do IAM, consulte Actions defined by AWS Organizations na Service Authorization Reference.

Ao combinar um `Action` e um `Resource` em uma única política de permissão `Statement`, você controla exatamente em quais recursos determinado conjunto de ações pode ser usado.

Chaves de condição

A AWS fornece chaves de condição que você pode consultar para fornecer controle granular aprimorado sobre determinadas ações. Você pode referenciar essas chaves de condição no elemento `Condition` de uma política do IAM para especificar as circunstâncias adicionais necessárias para que a instrução seja considerada uma correspondência.

As chaves de condição a seguir são especialmente úteis ao AWS Organizations:

- `aws:PrincipalOrgID` – Simplifica especificando o elemento `Principal` em uma política baseada em recursos. Essa chave global fornece uma alternativa à listagem de todos os IDs de conta para todas as Contas da AWS de uma organização. Em vez de listar todas as contas que são membros de uma organização, você pode especificar o ID da organização no elemento `Condition`.

  > **Note**
  >
  > Essa condição global também se aplica a conta de gerenciamento de uma organização.

Para obter mais informações, consulte a descrição das chaves de contexto de condição AWS global `PrincipalOrgID` no Guia do usuário do IAM.

- `aws:PrincipalOrgPaths` – Use essa chave de condição para corresponder membros de uma determinada raiz de organização, uma UO ou suas subordinadas. A chave de condição `aws:PrincipalOrgPaths` retorna true (verdadeiro) quando o usuário principal (usuário-raiz, usuário do IAM ou função do IAM) que faz a solicitação está no caminho da organização especificado. Um caminho é uma representação de texto da estrutura de uma entidade do AWS Organizations. Para obter mais informações sobre caminhos, consulte Entenda o caminho da AWS Organizations entidade no Guia do usuário do IAM. Para obter mais informações sobre o uso dessa chave de condição, consulte aws: PrincipalOrgPaths no Guia do usuário do IAM.

  Por exemplo, o seguinte elemento de condição é correspondido para membros de qualquer uma das duas OUs na mesma organização.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "aws:PrincipalOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
        ]
    }
}
```

- `organizations:PolicyType` – Você pode usar essa chave de condição para restringir as operações de API relacionadas a políticas do Organizations para funcionar apenas nas políticas do Organizations do tipo especificado. É possível aplicar essa chave de condição a qualquer instrução de política que inclua uma ação que interaja com as políticas do Organizations.

  Você pode usar os seguintes valores com essa chave de condição:

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_POLICY`

  Por exemplo, a política do exemplo a seguir permite que o usuário execute qualquer operação do Organizations. No entanto, se o usuário executar uma operação que usa um argumento de

política, a operação só será permitida se a política especificada for uma política de marcação. A operação falha se o usuário especificar qualquer outro tipo de política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal`— Disponível como condição se você usar as AWSServiceAccess operações Ativar AWSServiceAccess ou Desativar para ativar ou desativar o acesso confiável com outros AWS serviços. Você pode usar o `organizations:ServicePrincipal` para restringir as solicitações feitas por essas operações para uma lista de nomes principais de serviços aprovados.

  Por exemplo, a política a seguir permite que o usuário especifique apenas o AWS Firewall Manager ao habilitar e a desabilitar acesso confiável com o AWS Organizations:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
```

```
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

Para ver uma lista de todas as chaves de condição AWS Organizations específicas que podem ser usadas como permissões em uma política do IAM, consulte Chaves de condição AWS Organizations na Referência de autorização de serviço.

## Informações sobre propriedade de recursos

A Conta da AWS possui os recursos criados na conta, independentemente de quem os criou. Mais especificamente, o proprietário do recurso é a Conta da AWS da entidade principal (ou seja, o usuário raiz, um usuário do IAM ou um perfil do IAM) que autentica a solicitação de criação de recursos. Para uma organização da AWS, é sempre a conta de gerenciamento. Você não pode chamar a maioria das operações que criam ou acessam recursos da organização das contas dos membros. Os seguintes exemplos mostram como isso funciona:

- Se você usar as credenciais da conta-raiz da sua conta de gerenciamento para criar uma UO, sua conta de gerenciamento será a proprietária do recurso. (Em AWS Organizations, o recurso é a UO.)
- Se você criar um usuário do IAM em sua conta de gerenciamento e conceder permissões para criar uma UO para esse usuário, o usuário poderá criar uma UO. No entanto, a conta de gerenciamento à qual o usuário pertence é a proprietária do recurso da UO.
- Se você criar uma função do IAM na sua conta de gerenciamento com permissões para criar uma UO, qualquer pessoa que possa assumir a função pode criar uma UO. A conta de gerenciamento, à qual pertence a função (não o usuário que assume a função), é a proprietária do recurso da UO.

## Gerenciamento de acesso aos recursos

A política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação de políticas de permissões.

> **Note**
>
> Esta seção discute o uso do IAM no contexto do AWS Organizations. Não são fornecidas informações detalhadas sobre o serviço IAM. Para concluir a documentação do IAM, consulte o Guia do usuário do IAM. Para obter informações sobre a sintaxe e as descrições das políticas do IAM, consulte a referência da política JSON do IAM no Guia do usuário do IAM.

As políticas anexadas a uma identidade do IAM são chamadas de políticas baseadas em identidade (políticas do IAM). As políticas anexadas a um recurso são conhecidas como políticas baseadas em recurso. O AWS Organizations suporta apenas políticas baseadas em identidade (políticas do IAM).

Tópicos

- Políticas de permissão baseadas em identidade (políticas do IAM)
- Políticas baseadas em recurso

Políticas de permissão baseadas em identidade (políticas do IAM)

Você pode anexar políticas a identidades do IAM para permitir que essas identidades executem operações em recursos da AWS. Por exemplo, você pode fazer o seguinte:

- Anexar uma política de permissões a um usuário ou grupo em sua conta: para conceder a um usuário permissões para criar um recurso do AWS Organizations, como uma política de controle de serviço (SCP) ou uma UO, você pode anexar uma política de permissões a um usuário ou a um grupo ao qual o usuário pertence. O usuário ou grupo deve estar na conta de gerenciamento da organização.
- Anexar uma política de permissões a uma função (grant cross-account permissions) – Você pode anexar uma política de permissões baseadas em identidade a uma função do IAM para conceder acesso entre contas a uma organização. Por exemplo, o administrador na conta de gerenciamento pode criar uma função para conceder permissões entre contas para um usuário da conta-membro, da seguinte forma:
  1. O administrador da conta de gerenciamento cria uma função do IAM e anexa uma política de permissões à função que concede permissões aos recursos da organização.
  2. O administrador da conta de gerenciamento anexa uma política de confiança para a função que identifica o ID da conta do membro como `Principal`, que pode assumir a função.

3. O administrador da conta do membro pode então delegar permissões para assumir a função a quaisquer usuários na conta do membro. Isso permite que os usuários na conta do membro criem ou acessem recursos na conta de gerenciamento e na organização. O principal da política de confiança também pode ser o principal de um serviço da AWS, se você desejar conceder permissões para um serviço da AWS para assumir a função.

Para obter mais informações sobre o uso do IAM para delegar permissões, consulte Gerenciamento de acesso no Manual do usuário do IAM.

A seguir estão exemplos de políticas que permitem ao usuário executar a ação `CreateAccount` na organização:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

Você também pode fornecer um ARN parcial no elemento `Resource` da política para indicar o tipo de recurso.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

Você também pode negar a criação de contas que não incluam tags específicas para a conta que está sendo criada.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

Para obter mais informações sobre usuários, grupos, funções e permissões, consulte identidades do IAM (usuários, grupos de usuários e funções) no Guia do usuário do IAM.

Políticas baseadas em recurso

Alguns serviços, como o Amazon S3, suportam políticas de permissões baseadas em recursos. Por exemplo, você pode anexar uma política a um bucket do Amazon S3 para gerenciar permissões de acesso a esse bucket. O AWS Organizations não suporta políticas baseadas em recursos no momento.

## Especificação de elementos da política: ações, condições, efeitos e recursos

Para cada recurso do AWS Organizations, o serviço define um conjunto de operações de API, ou ações, capazes de interagir com ou manipular esse recurso de alguma forma. Para conceder permissões a essas operações da API, o AWS Organizations define um conjunto de ações que podem ser especificadas em uma política. Por exemplo, para o recurso UO, o AWS Organizations define ações como as seguintes:

- `AttachPolicy` e `DetachPolicy`
- `CreateOrganizationalUnit` e `DeleteOrganizationalUnit`

- `ListOrganizationalUnits` e `DescribeOrganizationalUnit`

Em alguns casos, a execução de uma operação de API pode exigir permissões para mais de uma ação e mais permissões para mais de um recurso.

Veja a seguir mais elementos básicos que você pode usar em uma política de permissão do IAM:

- Action (Ação) – Use essa palavra-chave para identificar as operações (ações) que deseja permitir ou negar. Por exemplo, dependendo do `Effect` especificado, o `organizations:CreateAccount` permite ou nega as permissões de usuário para executar a operação `CreateAccount` do AWS Organizations. Para obter mais informações, consulte Elementos da política JSON do IAM: ação no Guia do usuário do IAM.
- Resource (Recurso) – Use essa palavra-chave para especificar o ARN do recurso ao qual a instrução da política se aplica. Para obter mais informações, consulte Elementos da política JSON do IAM: recurso no Guia do usuário do IAM.
- Condition (Condição) – Use essa palavra-chave para especificar uma condição que deve ser atendida para que a instrução da política seja aplicável. `Condition` normalmente especifica circunstâncias adicionais que devem ser atendidas para que a política seja uma correspondência. Para obter mais informações, consulte Elementos de política JSON do IAM: Condição no Manual do usuário do IAM.
- Effect (Efeito) – Use essa palavra-chave para especificar se a instrução da política permite ou nega a ação no recurso. Se você não conceder (ou permitir) explicitamente o acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar explicitamente acesso a um recurso, o que pode fazer para garantir que o usuário não execute a ação especificada no recurso especificado, mesmo se uma política diferente conceder acesso. Para obter mais informações, consulte Elementos da política JSON do IAM: efeito no Guia do usuário do IAM.
- Principal – Em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política está anexada é automática e implicitamente o principal. Para as políticas baseadas em recursos, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (aplica-se somente a políticas baseadas em recursos). O AWS Organizations atualmente dá suporte somente a políticas baseadas em identidade, não com políticas baseadas em recursos.

Para saber mais sobre a sintaxe e as descrições das políticas do IAM, consulte a referência da política JSON do IAM no Guia do usuário do IAM.

# Uso de políticas baseadas em identidade (políticas do IAM) para o AWS Organizations

Como administrador da conta de gerenciamento de uma organização, você pode controlar o acesso a recursos da AWS, anexando políticas de permissões a identidades do AWS Identity and Access Management (IAM) (usuários, grupos e funções) dentro da organização. Ao conceder permissões, você decide quem recebe as permissões, os recursos relacionados às permissões concedidas e as ações específicas que deseja permitir nesses recursos. Se as permissões forem concedidas a uma função, essa função poderá ser assumida por usuários em outras contas na organização.

Por padrão, um usuário não tem nenhum tipo de permissão. Todas as permissões devem ser explicitamente concedidas por uma política. Se uma permissão não for explicitamente concedida, será implicitamente negada. Se uma permissão for explicitamente negada, substituirá qualquer outra política que possa tê-la permitido. Em outras palavras, um usuário tem apenas as permissões que são explicitamente concedidas e que não são explicitamente negadas.

Além das técnicas básicas descritas neste tópico, você pode controlar o acesso à sua organização usando as tags aplicadas aos recursos de sua organização: a raiz da organização, unidades organizacionais (UO), contas e políticas. Para ter mais informações, consulte Controle de acesso baseado em atributo com tags e AWS Organizations.

## Concessão de permissões administrativas completas a um usuário

Você pode criar uma política do IAM que concede permissões completas de administrador do AWS Organizations a um usuário do IAM na sua organização. Você pode fazer isso no editor de políticas JSON no console do IAM.

Para usar o editor de políticas JSON para criar uma política

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Policies (Políticas).

   Se essa for a primeira vez que você escolhe Políticas, a página Bem-vindo às políticas gerenciadas será exibida. Escolha Conceitos básicos.
3. Na parte superior da página, escolha Criar política.
4. Na seção Editor de políticas, escolha a opção JSON.
5. Insira o seguinte documento de política JSON:

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

6. Escolha Próximo.

> **Note**
>
> É possível alternar entre as opções de editor Visual e JSON a qualquer momento. Porém, se você fizer alterações ou escolher Próximo no editor Visual, o IAM poderá reestruturar a política a fim de otimizá-la para o editor visual. Para obter mais informações, consulte Restruturação de política no Guia do usuário do IAM.

7. Na página Revisar e criar, insira um Nome de política e uma Descrição (opcional) para a política que você está criando. Revise Permissões definidas nessa política para ver as permissões que são concedidas pela política.
8. Escolha Criar política para salvar sua nova política.

Para saber mais sobre como criar uma política do IAM, consulte Como criar políticas do IAM no Guia do usuário do IAM.

## Concessão de acesso limitado por ações

Se você deseja conceder permissões limitadas, em vez de permissões completas, pode criar uma política que relaciona as permissões individuais que deseja conceder no elemento `Action` da política de permissões do IAM. Como mostrado no exemplo a seguir, você pode usar caracteres curinga (*) para conceder somente as permissões `Describe*` e `List*`, basicamente fornecendo acesso somente leitura para a organização.

> **Note**
>
> Em uma política de controle de serviço (SCP), o caractere curinga (*) em um elemento `Action` pode ser usado somente sozinho ou no fim da string. Ele não pode aparecer

no início nem no meio da string. Portanto, `"servicename:action*"` é válido, mas `"servicename:*action"` e `"servicename:some*action"` são inválidos em SCPs.

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

Para ver uma lista de todas as permissões que estão disponíveis para atribuição em uma política do IAM, consulte Actions defined by AWS Organizations na Referência de Autorização de Serviço.

## Concessão de acesso a recursos específicos

Além de restringir o acesso a ações específicas, você pode restringir o acesso a entidades específicas em sua organização. Os elementos `Resource` nos exemplos nas seções anteriores especificam o caractere curinga ("*"), que significa "qualquer recurso que a ação pode acessar." Em vez disso, é possível substituir "*" pelo Nome de recurso da Amazon (ARN) de entidades específicas para as quais você deseja permitir o acesso.

Exemplo: concessão de permissões para uma única UO

A primeira instrução da política a seguir permite que um usuário do IAM tenha acesso de leitura a toda a organização, mas a segunda instrução permite que o usuário execute ações administrativas do AWS Organizations apenas em uma unidade organizacional (UO) especificada. Isso não se estende a qualquer UO subordinada. Nenhum acesso de cobrança é concedido. Observe que isso não concede acesso administrativo às Contas da AWS na UO. Concede apenas permissões para executar operações do AWS Organizations nas contas dentro da UO especificada:

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

```
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
    }
  ]
}
```

Você obtém os IDs da UO e da organização no console do AWS Organizations ou chamando as APIs `List*`. O usuário ou grupo ao qual você aplica essa política pode realizar qualquer ação (`"organizations:*"`) em qualquer entidade que seja contida diretamente pela UO especificada. A UO é identificada pelo Nome de recurso da Amazon (ARN).

Para obter mais informações sobre os ARNs de vários recursos, consulte Tipos de recursos definidos por AWS Organizations na Referência de Autorização de Serviço.

## Concessão da capacidade de habilitar acesso confiável para entidades de serviço primárias limitadas

Você pode usar o elemento `Condition` de uma declaração de política para limitar ainda mais as circunstâncias em que a declaração de política é correspondente.

Exemplo: conceder permissões para habilitar acesso confiável para um serviço especificado

A declaração a seguir mostra como você pode restringir a capacidade para habilitar acesso confiável apenas aos serviços que você especificar. Se o usuário tentar chamar a API com um principal de serviço diferente do principal do AWS IAM Identity Center, essa política não será correspondente e a solicitação será negada:

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

```
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

Para obter mais informações sobre os ARNs de vários recursos, consulte Tipos de recursos definidos por AWS Organizations na Referência de Autorização de Serviço.

## Controle de acesso baseado em atributo com tags e AWS Organizations

O controle de acesso baseado em atributos permite que você use atributos gerenciados pelo administrador, como tags anexadas a recursos da AWS e identidades da AWS, para controlar o acesso a esses recursos. Por exemplo, você pode especificar que um usuário pode acessar um recurso quando o usuário e o recurso tiverem o mesmo valor para uma determinada tag.

Os recursos marcáveis do AWS Organizations incluem Contas da AWS, a raiz, as unidades organizacionais (UOs) ou as políticas da organização. Quando anexa tags a recursos do Organizations, você pode usar essas tags para controlar quem pode acessar esses recursos. Para isso, adicione elementos `Condition` às instruções da política de permissões do AWS Identity and Access Management (IAM) que verificam se determinadas chaves e valores de tag estão presentes antes de permitir a ação. Isso permite que você crie uma política do IAM que diga efetivamente "Permitir que o usuário gerencie somente as UOs que têm uma tag com uma chave `X` e um valor `Y`" ou "Permitir que o usuário gerencie somente as UOs marcadas com uma chave `Z` que tem o mesmo valor da chave anexada ao usuário `Z`".

Você pode basear seus testes de `Condition` em diferentes tipos de referências de tag em uma política do IAM.

- Verificação das tags anexadas aos recursos especificados na solicitação
- Verificação de tags anexadas ao usuário ou à função do IAM que está fazendo a solicitação
- Verificar as tags que estão incluídas como parâmetros na solicitação

Para obter mais informações sobre o uso de tags para controle de acesso em políticas, consulte Controlar o acesso aos/de usuários e funções do IAM usando tags de recurso do IAM. Para obter a sintaxe completa das políticas de permissão do IAM, consulte a Referência de política JSON do IAM

### Verificação das tags anexadas aos recursos especificados na solicitação

Quando faz uma solicitação usando o AWS Management Console, o AWS Command Line Interface (AWS CLI) ou um dos AWS SDKs, você especifica os recursos que deseja acessar com essa solicitação. Se você estiver tentando listar os recursos de um determinado tipo disponíveis, ler ou gravar em um recurso, modificar ou atualizar um recurso, você especifica o recurso a ser acessado como um parâmetro na solicitação. Essas solicitações são controladas pelas políticas de permissões do IAM que você anexa aos seus usuários e funções. Nessas políticas, você pode comparar as tags anexadas ao recurso solicitado e optar por permitir ou negar acesso com base nas chaves e valores dessas tags.

Para verificar uma tag anexada ao recurso, você referencia a tag em um elemento do `Condition` prefaciando o nome da chave da tag com a seguinte sequência: `aws:ResourceTag/`

Por exemplo, o exemplo de política a seguir permite que o usuário ou a função execute qualquer operação do AWS Organizations a menos que esse recurso tenha uma tag com a chave `department` e o valor `security`. Se essa chave e valor estiverem presentes, a política nega explicitamente operação do `UntagResource`.

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
```

```
        }
    ]
}
```

Para obter mais informações sobre como usar esse elemento, consulte Controle de acesso a recurso e aws:ResourceTag no Manual do usuário do IAM.

### Verificação de tags anexadas ao usuário ou à função do IAM que está fazendo a solicitação

Você pode controlar o que a pessoa que está fazendo a solicitação (principal) tem permissão para fazer com base nas tags anexadas ao usuário ou à função do IAM dessa pessoa. Para fazer isso, use a chave de condição `aws:PrincipalTag/key-name` para especificar a tag e o valor que devem ser anexados ao usuário ou à função que está chamando.

O exemplo a seguir mostra como permitir uma ação apenas quando a tag especificada (`cost-center`) tiver o mesmo valor no usuário principal que chama a operação e no recurso que está sendo acessado pela operação. Neste exemplo, o usuário que chama só pode iniciar e interromper uma instância do Amazon EC2 se a instância estiver marcada com o mesmo valor `cost-center` que o usuário.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

Para obter mais informações sobre como usar esse elemento, consulte Controle de acesso dos usuários principais do IAM e `aws:PrincipalTag` no Manual do usuário do IAM.

## Verificar as tags que estão incluídas como parâmetros na solicitação

Várias operações permitem que você especifique tags como parte da solicitação. Por exemplo, ao criar um recurso, você pode especificar as tags anexadas ao novo recurso. Você pode especificar um elemento `Condition` que usa `aws:TagKeys` para permitir ou negar a operação baseado em se uma chave de tag específica, ou um conjunto de chaves, está incluída na solicitação. Este operador de comparação não se importa com o valor que a tag contém. Ele só verifica se uma tag com a chave especificada está presente.

Para verificar a chave de tag, ou uma lista de chaves, especifique um elemento `Condition` com a seguinte sintaxe:

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

Você pode usar `ForAllValues:` para prefaciar o operador de comparação para garantir que todas as chaves na solicitação devam corresponder a uma das chaves especificadas na política. Por exemplo, o exemplo de política a seguir só permite qualquer operação do Organizations se todas as três chaves de tags especificadas estiverem presentes na solicitação.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

Ou então, você pode usar `ForAnyValue:` para prefaciar o operador de comparação para garantir que pelo menos uma das chaves na solicitação deva corresponder a uma das chaves especificadas

na política. Por exemplo, o exemplo de política a seguir só permite uma operação do Organizations se pelo menos uma das chaves de tags especificadas estiverem presentes na solicitação.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}
```

Várias operações permitem especificar tags na solicitação. Por exemplo, ao criar um recurso, você pode especificar as tags anexadas ao novo recurso. É possível comparar um par de chave/valor na política com um par de chave/valor incluído na solicitação. Para fazer isso, referencie a tag em um elemento `Condition` prefaciando o nome da chave de tag com a seguinte sequência: `aws:RequestTag/`*`key-name`*, depois, especifique o valor da tag que deve estar presente.

Por exemplo, o exemplo de política a seguir nega qualquer solicitação do usuário ou da função para criar uma Conta da AWS na qual a solicitação não tenha a tag `costcenter`, ou forneça essa tag com um valor diferente de 1, 2 ou 3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
```

```
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

Para obter mais informações sobre como usar esses elementos, consulte aws:TagKeys e aws:RequestTag no Manual do usuário do IAM.

# Registrar em log e monitorar no AWS Organizations

Como uma prática recomendada, você deve monitorar a sua organização para garantir que as alterações sejam registradas. Isso ajuda a garantir que qualquer alteração inesperada possa ser investigada e alterações indesejadas possam ser restabelecidas. A AWS Organizations atualmente oferece suporte a dois serviços AWS que permitem que você monitore a sua organização e a atividade que acontece dentro dela.

Tópicos

- Registrar em log chamadas de API do AWS Organizations com o AWS CloudTrail
- Amazon EventBridge

## Registrar em log chamadas de API do AWS Organizations com o AWS CloudTrail

O AWS Organizations é integrado a AWS CloudTrail, serviço que fornece um registro das ações realizadas por um usuário, perfil ou AWS serviço em AWS Organizations. O CloudTrail captura

todas as chamadas de API para o AWS Organizations como eventos, incluindo as chamadas do console do AWS Organizations e de chamadas de código para APIs do AWS Organizations. Caso crie uma trilha, voce pode habilitar a entrega contínua de eventos CloudTrail para um bucket Amazon S3, inclusive eventos para AWS Organizations. Mesmo que não configure uma trilha, você ainda pode visualizar os eventos mais recentes no console CloudTrail em Histórico de Eventos. Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o AWS Organizations, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o AWS CloudTrail Guia de Usuário.

> **Important**
>
> Você pode visualizar todas as informações do CloudTrail para AWS Organizations apenas na região Leste dos EUA (Norte da Virgínia). Caso você não veja sua atividade do AWS Organizations no console do CloudTrail, defina seu console para US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)), usando o menu no canto superior direito. Se você consultar o CloudTrail com a AWS CLI ou ferramentas do SDK, direcione sua consulta para o endpoint Leste dos EUA (Norte da Virgínia).

## Informações do AWS Organizations no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade no AWS Organizations, ela é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS Organizations, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket Amazon S3. Quando o registro em log do CloudTrail está habilitado em sua Conta da AWS, as chamadas de API feitas para ações do AWS Organizations serão rastreadas nos arquivos de log do CloudTrail, onde serão gravadas com outros registros de serviço da AWS. Você pode configurar outros serviços da AWS para analisar e atuar mais profundamente sobre os dados de eventos coletados nos logs do CloudTrail. Para mais informações, consulte:

- Visão Geral para Criar uma Trilha

- Serviços e Integrações Compatíveis com CloudTrail
- Configurando Notificações Amazon SNS para CloudTrail

Todas as ações do AWS Organizations são registradas pelo CloudTrail e são documentadas na Referência de API do AWS Organizations. Por exemplo, as chamadas para `CreateAccount` (incluindo o evento `CreateAccountResult`), `ListHandshakesForAccount`, `CreatePolicy` e `InviteAccountToOrganization` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log contém informações sobre quem gerou a solicitação. As informações de identidade do usuário na entrada de log ajudam você a determinar o seguinte:

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

Para mais informações, consulte Elemento userIdentity CloudTrail.

## Noções básicas sobre entradas de arquivos de log do AWS Organizations

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

Exemplo de entrada de log: CloseAccount

O exemplo a seguir mostra uma entrada de log do CloudTrail para uma amostra de chamada de `CloseAccount` que é gerada quando a API é chamada e o fluxo de trabalho para encerrar a conta começa o processamento em segundo plano.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail para uma chamada de `CloseAccountResult` depois que o fluxo de trabalho em segundo plano para criar a conta é concluído com êxito.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
```

```
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

Exemplo de entrada de log: CreateAccount

O exemplo a seguir mostra uma entrada de log do CloudTrail para um exemplo de chamada de `CreateAccount` que é gerada quando a API é chamada e o fluxo de trabalho para criar a conta começa a processar em segundo plano.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail para uma chamada de `CreateAccount` depois que o fluxo de trabalho em segundo plano para criar a conta for concluído com êxito.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail para uma chamada de `CreateAccount` depois que o fluxo de trabalho em segundo plano falha ao criar a conta.

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
```

```
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

Exemplo de entrada de log: CreateOrganizationalUnit

O exemplo a seguir mostra uma entrada de log do CloudTrail para um exemplo de chamada de `CreateOrganizationalUnit`.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
```

```
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Exemplo de entrada de log: InviteAccountToOrganization

O exemplo a seguir mostra uma entrada de log do CloudTrail para um exemplo de chamada de `InviteAccountToOrganization`.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
```

```
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
```

```
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Exemplo de entrada de log: AttachPolicy

O exemplo a seguir mostra uma entrada de log do CloudTrail para um exemplo de chamada de `AttachPolicy`. A resposta indica que a chamada falhou porque o tipo de política solicitado não está ativado na raiz em que a solicitação de anexação foi empreendida.

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
```

```
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

## Amazon EventBridge

O AWS Organizations pode trabalhar com o Amazon EventBridge, anteriormente Amazon CloudWatch Events, para gerar eventos quando ações especificadas pelo administrador ocorrerem em uma organização. Por exemplo, devido à confidencialidade dessas ações, a maioria dos administradores desejarão ser avisados sempre que alguém criar uma nova conta na organização ou quando um administrador de uma conta membro tentar deixar a organização. Você pode configurar as regras do EventBridge para procurar essas ações e, em seguida, enviar os eventos gerados para destinos definidos pelo administrador. Os alvos podem ser um tópico do Amazon SNS que envia e-mails ou mensagens de texto a seus assinantes. Você também pode criar uma função do AWS Lambda que registra os detalhes da ação para análise posterior.

Para um tutorial que mostra como habilitar o EventBridge para monitorar as principais atividades em sua organização, consulte Tutorial: monitorar alterações importantes em sua organização com o Amazon EventBridge.

Para saber mais sobre o EventBridge, incluindo como configurá-lo e habilitá-lo, consulte o Guia do usuário do Amazon EventBridge.

# Validação de conformidade do AWS Organizations

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. 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 .

Sua responsabilidade de conformidade ao usar Serviços 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.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- 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— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- 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 AWS Organizations

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, altas taxas de transferência e em redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicativos e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

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

## Segurança da infraestrutura no AWS Organizations

Por ser um serviço gerenciado, o AWS Organizations é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o Organizations pela rede. Os clientes devem oferecer suporte para:

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

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

Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

# AWS OrganizationsReferência do

Use os tópicos nesta seção para localizar informações de referência detalhadas para diversos aspectos do AWS Organizations.

Tópicos



## Cotas para AWS Organizations

Esta seção especifica cotas que afetam o AWS Organizations.

### Diretrizes de nomenclatura

A seguir estão as diretrizes para nomes que você cria em AWS Organizations, incluindo nomes de contas, unidades organizacionais (OUs), raízes e políticas:

- Eles devem ser compostos por caracteres Unicode
- O comprimento máximo da sequência para nomes varia de acordo com o objeto. Para ver o limite real de cada um, consulte a Referência de API do AWS Organizations e localize a operação de API que cria o objeto. Veja os detalhes para o parâmetro `Name` dessa operação. Por exemplo: Account name (Nome da conta) ou UO name (Nome da UO).

### Valores máximo e mínimo

A seguir estão os valores máximos padrão para entidades em AWS Organizations.

> **Note**
>
> Você pode solicitar o aumento de alguns desses valores usando o console do Service Quotas.
> Organizations é um serviço global que está fisicamente hospedado na região Leste dos EUA (Norte da Virgínia) (`us-east-1`). Portanto, você deve usar `us-east-1` para acessar as cotas do Organizations ao usar o console Service Quotas, AWS CLI o ou AWS um SDK.

| | |
|---|---|
| Número de Contas da AWS em uma organização | 10: o número máximo padrão de contas permitidas em uma organização. Se precisar de mais, solicite um aumento usando o console do Service Quotas.<br><br>Um convite enviado para uma conta é contabilizado como uma cota. A contagem é revertida se a conta convidada recusa, a conta de gerenciamento cancela o convite ou a validade do convite expira.<br><br>As contas e organizações recém-criadas podem ter uma cota abaixo do padrão de 10 contas. |
| Número de raízes em uma organização | 1 |
| Número de UOs em uma organização | 1000 |
| Número de políticas de cada tipo em uma organização | Políticas de exclusão de serviços de IA: 1000<br><br>Políticas de backup: 1000<br><br>Políticas de controle de serviços: 2000<br><br>Políticas de tags: 1000 |
| Tamanho máximo de um documento de política | Políticas de exclusão de serviços de IA: 2500 caracteres<br><br>Políticas de backup: 10.000 caracteres<br><br>Políticas de controle de serviço: 5120 caracteres<br><br>Políticas de tag: 10.000 caracteres<br><br>Observação: se você salvar a política usando o AWS Management Console, o espaço em branco extra (como espaços e quebras de linha) entre elementos JSON e fora das aspas será removido e não contado. Se você salvar a política usando uma operação do SDK ou a AWS CLI, a política será salva exatamente como você forneceu e nenhuma remoção automática de caracteres ocorrerá. |

| | |
|---|---|
| Aninhamento máximo UO em uma raiz | Cinco níveis de profundidade de UOs em uma raiz. |
| O número máximo de tentativas de convite que você pode realizar em um período de 24 horas | 20 ou o número máximo de contas permitidas na sua organização, o que for maior. Os convites aceitos não são considerados nessa cota. Assim que um convite é aceito, você pode enviar outro convite no mesmo dia.<br><br>Se o número máximo de contas permitido na sua organização for inferior a 20, você receberá uma exceção de "account limit exceeded (limite de conta excedido)" se tentar convidar mais contas do que a sua organização pode comportar. No entanto, você pode cancelar convites e enviar novos até o máximo de 20 tentativas em um dia. |
| Número de contas-membros que você pode criar simultaneamente | 5 — Assim que uma é concluída, você pode iniciar outra, mas apenas cinco podem estar em andamento de cada vez. |
| Número de contas-membros que você pode encerrar em um período de 30 dias | 10% das contas dos membros em uma organização, com um máximo de 1000.<br><br>• < 100 contas — Você pode fechar até 10 contas de membros<br>• 100 a 10.000 contas — Você pode fechar até 10% de suas contas de membros<br>• > 10.000 contas — Você pode fechar até 1000 contas de membros<br><br>Por exemplo, se você tiver 10.500 contas de membros, poderá fechar até 1.000 (não 1050) contas em um período de 30 dias. Depois de atingir essa cota, você pode fechar contas adicionais noAWS Billing console ou aguardar até que sua cota seja redefinida. Para obter mais informações, consulte O que você precisa saber antes de fechar sua AWS conta no Guia de gerenciamento de contas. |
| Número de contas-membros que você pode encerrar simultaneamente | Três: só é possível ter três encerramentos de conta em andamento ao mesmo tempo. Assim que o processamento de uma terminar, você pode encerrar outra conta. |

| | |
|---|---|
| Número de entidades às quais você pode anexar uma política | Ilimitado |
| Número de tags que você pode anexar a uma raiz, UO ou conta | 50 |
| Tamanho máximo da política de delegação baseada em recursos | 40 mil caracteres |

## Tempos de expiração para handshakes

A seguir estão os tempos limite para apertos de mão. AWS Organizations

| | |
|---|---|
| Convite para participar de uma organização | 15 dias |
| Solicitação para ativar todos os recursos em uma organização | 90 dias |
| O handshake é excluído e não aparece mais em listas | 30 dias após a conclusão do handshake |

## Número de políticas que você pode anexar a uma entidade

O mínimo e o máximo dependem do tipo de política e da entidade à qual você está anexando a política. A tabela a seguir mostra cada tipo de política e o número de entidades às quais você pode anexar cada tipo.

> **Note**
>
> Esses números se aplicam somente às políticas diretamente vinculadas a uma UO ou a uma conta. Políticas que afetam uma UO ou conta por herança não contam para esses limites.

| Tipo de política | Mínimo anexado a uma entidade | Máximo anexado à raiz | Máximo anexado por UO | Máximo anexado por conta |
|---|---|---|---|---|
| Política de controle de serviço | 1 — Cada entidade deve ter sempre pelo menos uma SCP anexada. Não é possível remover a última SCP de uma entidade. | 5 | 5 | 5 |
| Política de exclusão dos serviços de IA | 0 | 5 | 5 | 5 |
| Política de backup | 0 | 10 | 10 | 10 |
| Política de tag | 0 | 10 | 10 | 10 |

> **Note**
>
> No momento, você pode ter apenas uma raiz em uma organização.

## Limites de controle de utilização

A tabela a seguir lista as AWS Organizations APIs por categoria de gerenciamento e mostra suas respectivas taxas de aceleração no nível da conta e da organização.

| AWS Organizations API | Limite por conta (taxa, pico) | Limite por organização (taxa, pico) |
|---|---|---|
| Gerenciamento de contas | | |
| CloseAccount | 0,5, 1 | |
| CreateAccount, CreateGovCloudAccount | 0,1, 3 | |
| DescribeAccount | 20, 30 | 24, 36 |
| DescribeCreateAccountStatus | 2, 2 | 2, 3 |
| LeaveOrganization | 1, 1 | |
| ListCreateAccountStatus | 5, 8 | 6, 10 |
| Gerenciamento de aperto de mão | | |
| AcceptHandshake, DescribeHandshake | 1, 1 | |
| CancelHandshake | 2, 3 | |
| DeclineHandshake | 1, 3 | |
| InviteAccountToOrganization | 3, 5 | |
| ListHandshakesForAccount, ListHandshakesForOrganization | 5, 8 | 6, 10 |
| Gestão da organização | | |
| CreateOrganization, DeleteOrganization, EnableFullControl | 1, 1 | |
| CreateOrganizationalUnit, DescribeOrganization | 1, 2 | |

| AWS Organizations API | Limite por conta (taxa, pico) | Limite por organização (taxa, pico) |
|---|---|---|
| MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit | 2, 3 | |
| DescribeOrganizationalUnit | 2, 2 | 2, 3 |
| ListAccounts | 8, 12 | 9, 15 |
| ListChildren | 6, 10 | 7, 12 |
| ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent | 5, 8 | 6, 10 |
| ListRoots | 1, 2 | 1, 3 |
| ListTagsForResource | 10, 15 | 12, 18 |
| RemoveAccountFromOrganization | 2, 2 | |
| TagResource, UntagResource | 4, 6 | |
| Gerenciamento de políticas | | |
| CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy | 2, 3 | |
| DescribePolicy | 2, 2 | 2, 3 |
| DisablePolicyType, EnablePolicyType | 1, 1 | |
| ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy | 5, 8 | 6, 10 |
| UpdatePolicy | 2, 3 | |

| AWS Organizations API | Limite por conta (taxa, pico) | Limite por organização (taxa, pico) |
|---|---|---|
| Gerenciamento de serviços | | |
| AtivarAWSServiceAccess, desativar AWSServiceAccess | 1, 2 | |
| ListaAWSServiceAccessForOrganization, ListDelegatedServicesForAccount | 1, 3 | 1, 4 |
| ListDelegatedAdministrators | 5, 8 | 6, 10 |
| RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator | 1, 2 | |

# Políticas gerenciadas da AWS disponíveis para uso com o AWS Organizations

Esta seção identifica as políticas gerenciadas pela AWS, são fornecidas para você gerenciar sua organização. Você não pode modificar nem excluir uma política gerenciada da AWS, mas pode anexá-las ou separá-las para entidades de sua organização, conforme a necessidade.

## Políticas gerenciadas pela AWS Organizations para uso com o AWS Identity and Access Management (IAM)

Uma política gerenciada do IAM é fornecida e mantida pela AWS. Uma política gerenciada fornece permissões para tarefas comuns que você pode atribuir aos usuários anexando a política gerenciada ao usuário ou objeto de função apropriado do IAM. Você não precisa escrever a política você mesmo e, quando a AWS atualiza a política, conforme apropriado, para oferecer suporte a novos serviços, você obtém automaticamente e imediatamente o benefício da atualização. Você pode ver a lista de políticas gerenciadas pela AWS na página Policies (Políticas) no console do IAM. Use o menu suspenso Políticas de filtro para selecionar AWS gerenciado.

Você pode usar as seguintes políticas gerenciadas para conceder permissões a usuários da sua organização.

| Nome da política | Descrição | ARN |
| --- | --- | --- |
| AWSOrganizationsFullAccess | Fornece todas as permissões necessárias para criar e administrar totalmente uma organização. O conteúdo desta declaração de política é mostrado no seguinte trecho: | arn:aws:iam: :aws:policy/AWSOrganizationsFullAccess |

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSOrgan
izationsFullAccess",
            "Effect": "Allow",
            "Action":
 "organizations:*",
            "Resource": "*"
        },
        {
            "Sid": "AWSOrgan
izationsFullAccess
Account",
            "Effect": "Allow",
            "Action": [
                "account:
PutAlternateContact",
                "account:
DeleteAlternateContact",
                "account:
GetAlternateContact",
                "account:
GetContactInformation",
                "account:
PutContactInformation",
                "account:
ListRegions",
```

| Nome da política | Descrição | ARN |
| --- | --- | --- |

```
                "account:
EnableRegion",
                "account:
DisableRegion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSOrgan
izationsFullAccessCreateSLR
",
            "Effect": "Allow",
            "Action":
 "iam:CreateServiceLinkedRol
e",
            "Resource": "*",
            "Condition": {
                "StringEq
uals": {
                    "iam:AWSS
erviceName": "organiza
tions.amazonaws.com"
                }
            }
        }
    ]
}
```

| Nome da política | Descrição | ARN |
| --- | --- | --- |
| AWSOrganizationsReadOnlyAccess | Fornece acesso somente de leitura a informações sobre a organização. Não permite que o usuário faça nenhuma alteração. O conteúdo desta declaração de política é mostrado no seguinte trecho: | arn:aws:iam: :aws:policy/AWSOrganizationsReadOnlyAccess |

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSOrganizationsReadOnly",
         "Effect":"Allow",
         "Action":[
            "organizations:Describe*",
            "organizations:List*"
         ],
         "Resource": "*"
      },
      {
         "Sid": "AWSOrganizationsReadOnlyAccount",
         "Effect":"Allow",
         "Action":[
            "account:GetAlternateContact",
            "account:GetContactInformation",
            "account:ListRegions"
         ],
         "Resource": "*"
      }
   ]
}
```

## Atualizações em políticas gerenciadas pela AWS do Organizations

A tabela a seguir detalha as atualizações em políticas gerenciadas pela AWS desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações realizadas nesta página, inscreva-se no feed RSS na página Histórico de documentos do AWS Organizations.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSOrganizationsFullAccess— atualizado para incluir `Sid` elementos que descrevam a declaração de política. | Organizations adicionou `Sid` elementos para a política `AWSOrganizationsFullAccess` gerenciada. | 6 de fevereiro de 2024 |
| AWSOrganizationsReadOnlyAccess— atualizado para incluir `Sid` elementos que descrevam a declaração de política. | Organizations adicionou `Sid` elementos para a política `AWSOrganizationsReadOnlyAccess` gerenciada. | 6 de fevereiro de 2024 |
| AWSOrganizationsFullAccess— atualizado para permitir que as permissões da API da conta sejam ativadas ou desativadas Regiões da AWS por meio do console do Organizations. | O Organizations adicionou as ações `account:ListRegions` , `account:EnableRegion` e `account:DisableRegion` à política para habilitar o acesso de gravação para habilitar ou desabilitar regiões para uma conta. | 22 de dezembro de 2022 |
| AWSOrganizationsReadOnlyAccess— atualizado para permitir que as permissões de API da conta sejam listadas Regiões da AWS por meio do console do Organizations. | O Organizations adicionou a ação `account:ListRegions` à política para habilitar o acesso de visualização de regiões para uma conta. | 22 de dezembro de 2022 |
| AWSOrganizationsFullAccess— atualizado para permitir as permissões de API da conta necessárias para adicionar ou editar | O Organizations adicionou as ações `account:GetContactInformation` e `account:PutContactInformation` à política para habilitar acesso de | 21 de outubro de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| contatos da conta por meio do console do Organizations. | gravação a fim de modificar contatos de uma conta. | |
| AWSOrganizationsReadOnlyAccess— atualizado para permitir as permissões de API da conta necessárias para visualizar os contatos da conta por meio do console do Organizations. | O Organizations adicionou a ação `account:GetContactInformation` à política para habilitar acesso de visualização de contatos de uma conta. | 21 de outubro de 2022 |
| AWSOrganizationsFullAccess— atualizado para permitir a criação de uma organização. | O Organizations adicionou a permissão `CreateServiceLinkedRole` à política para habilitar a criação da função vinculada ao serviço, necessária para criar uma organização. A permissão é restrita à criação de uma função que pode ser usada somente pelo serviço `organizations.amazonaws.com` . | 24 de agosto de 2022 |
| AWSOrganizationsFullAccess— atualizado para permitir as permissões da API da conta necessárias para adicionar, editar ou excluir contatos alternativos da conta por meio do console do Organizations. | O Organizations adicionou as ações `account:GetAlternateContact` , `account:DeleteAlternateContact` e `account:PutAlternateContact` à política para habilitar acesso de gravação para modificar contatos alternativos de uma conta. | 7 de fevereiro de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSOrganizationsReadOnlyAccess— atualizado para permitir as permissões de API da conta necessárias para visualizar contatos alternativos da conta por meio do console do Organizations. | O Organizations adicionou a ação `account:GetAlternateContact` à política para habilitar acesso de visualização de contatos alternativos de uma conta. | 7 de fevereiro de 2022 |

## Políticas de controle de serviço gerenciadas pelo AWS Organizations

Políticas de controle de serviço (SCPs) são semelhantes às políticas de permissão do IAM, mas são um recurso do AWS Organizations, e não do IAM. Você usa SCPs para especificar o número máximo de permissões para entidades afetadas. Você pode anexar SCPs a raízes, unidades organizacionais (UOs) ou contas de sua organização. Você pode criar suas próprias ou usar as políticas definidas pelo IAM. Você pode ver a lista de políticas de sua organização na página Policies (Políticas) no console do Organizations.

> **Important**
>
> Cada raiz, UO e conta devem ter pelo menos uma SCP anexada durante todo o tempo.

| Nome da política | Descrição | ARN |
| --- | --- | --- |
| Completo AWSAccess | Fornece à conta de gerenciamento do AWS Organizations acesso às contas-membro. | arn:aws:organizations: :aws:policy/service_control_policy/p-FullAWSAccess |

# Solução de problemas do AWS Organizations

Se você encontrar problemas ao trabalhar com AWS Organizations, consulte os tópicos desta seção.

Tópicos



## Solução de problemas gerais

Use as informações contidas aqui para ajudar a diagnosticar e corrigir acesso negado ou outros problemas comuns que você pode encontrar ao trabalhar com o AWS Organizations.

Tópicos

## Eu recebo uma mensagem de "acesso negado" quando faço uma solicitação para o AWS Organizations

- Verifique se você tem permissões para chamar a ação e o recurso que solicitou. Um administrador deve conceder permissões anexando uma política do IAM ao seu usuário, grupo ou perfil. Se as declarações de política que concedem essas permissões incluírem condições, como horário do dia ou restrições de endereço IP, você também deverá cumprir esses requisitos ao enviar a solicitação. Para obter informações sobre como visualizar ou modificar políticas para um usuário, grupo ou perfil, consulte Trabalhar com políticas no Guia do usuário do IAM.
- Se você assinar solicitações de API manualmente (sem usar os AWS SDKs), verifique se assinou a solicitação corretamente.

## Eu recebo uma mensagem de "acesso negado" quando faço uma solicitação com credenciais de segurança temporárias

- Verifique se o usuário ou a função do que você está usando para fazer a solicitação tem as permissões corretas. As permissões para credenciais de segurança temporárias são derivadas de um usuário ou função do , para que as permissões sejam limitadas àquelas concedidas ao usuário ou função do . Para obter mais informações sobre como as permissões de credenciais de segurança temporárias são determinadas, consulte Controle de permissões para credenciais de segurança temporárias no Manual do usuário do IAM.
- Verifique se suas solicitações estão sendo assinadas corretamente e se a solicitação está bem formulada. Para obter detalhes, consulte a documentação do toolkit para o SDK escolhido ou Uso de credenciais de segurança temporárias para solicitar acesso aos recursos da AWS no Manual do usuário do IAM.
- Verifique se suas credenciais de segurança temporárias não expiraram. Para obter mais informações, consulte Solicitação de credenciais de segurança temporárias no Manual do usuário do IAM.

## Eu recebo uma mensagem de "acesso negado" quando tento deixar uma organização como uma conta-membro ou remover uma conta-membro como a conta de gerenciamento

- Você só pode remover uma conta-membro depois de habilitar o acesso de usuários do IAM da faturamento na conta-membro. Para obter mais informações, consulte Ativação de acesso ao console do Billing and Cost Management no Manual do usuário do AWS Billing.
- Você pode remover uma conta de sua organização somente se a conta tem as informações necessárias para operar como uma conta independente. Quando você cria uma conta em uma organização usando o console do AWS Organizations, a API ou os comandos da AWS CLI, essas informações não são coletadas automaticamente. Para uma conta que você desejar tornar independente, será necessário primeiro aceitar o Contrato de cliente da AWS, escolher um plano de suporte, fornecer e confirmar as informações de contato exigidas, bem como informar o método de pagamento atual. A AWS usa o método de pagamento para cobrar qualquer atividade da AWS faturável (fora do nível gratuito) AWS que ocorra enquanto a conta não está associada a uma organização. Para obter mais informações, consulte Sair de uma organização com sua conta-membro.

## Recebo uma mensagem "cota excedida" ao tentar adicionar uma conta à minha organização

Há um número máximo de contas que você pode ter em uma organização. Contas excluídas ou encerradas continuam contando em relação a essa cota.

Um convite para unir contas em relação ao número máximo de contas em sua organização. A contagem é revertida se a conta convidada recusa, a conta de gerenciamento cancela o convite ou a validade do convite expira.

- Antes de fechar ou excluir uma Conta da AWS, remova-a de sua organização, para que ela não continue a contar para a sua cota.
- Consulte Valores máximo e mínimo para obter mais informações sobre como solicitar um aumento de cota. .

## Recebi uma mensagem "esta operação exige um período de espera" ao adicionar ou remover contas

Algumas ações exigem um período de espera. Por exemplo, não é possível remover contas recém-criadas. Tente fazer isso novamente em alguns dias. Se você enfrentar problemas com cotas de contas ao adicionar e remover contas, consulte Valores máximo e mínimo para obter informações sobre como solicitar um aumento de cota.

## Recebo uma mensagem "a organização ainda está sendo inicializada" ao tentar adicionar uma conta à minha organização

Se receber esse erro, e já fizer mais de uma hora que criou a organização, entre em contato com o AWS Support.

## Recebo uma mensagem "Invitations are disabled" (Os convites estão desabilitados) quando tento convidar uma conta para a minha organização.

Isso acontece quando você habilita todos os recursos na sua organização. Esta operação pode levar algum tempo e requer que todas as contas-membro respondam. Até que a operação seja concluída, você não pode convidar novas contas para ingressar na organização.

## As alterações que eu faço nem sempre ficam imediatamente visíveis

Como um serviço que é acessado por meio de computadores em datacenters em todo o mundo, o AWS Organizations usa um modelo de computação distribuído chamado consistência eventual. Qualquer alteração feita no AWS Organizations leva tempo para se tornar visível em todos os endpoints possíveis. Esse atraso resulta, em parte, do tempo necessário para enviar os dados de um servidor para outro ou de uma zona de replicação para outra. O AWS Organizations também usa o armazenamento em cache para melhorar a performance, mas em alguns casos isso pode levar tempo. A alteração talvez não fique visível enquanto os dados armazenados em cache anteriormente não atingirem o tempo limite.

Projete seus aplicativos globais para compensar esses possíveis atrasos e garantir o funcionamento esperado, mesmo quando uma alteração feita em um local não fique imediatamente visível em outro.

Para obter mais informações sobre como alguns outros serviços da AWS são afetados por isso, consulte os seguintes recursos:

- Gerenciamento da consistência de dados no Guia do desenvolvedor de banco de dados do Amazon Redshift
- Modelo de consistência de dados do Amazon S3 no Manual do usuário do Amazon Simple Storage Service
- Garantia de consistência ao usar o Amazon S3 e o Amazon Elastic MapReduce para fluxos de trabalho ETL no blog sobre big data da AWS
- Consistência final do EC2 na Referência de API do Amazon EC2.

# Solução de problemas de políticas do AWS Organizations

Use as informações aqui para ajudar no diagnostico e na correção de erros comuns encontrados nas políticas do AWS Organizations.

## Políticas de controle de serviço

Políticas de controle de serviço (SCPs) no AWS Organizations são parecidas com as políticas do IAM e têm uma sintaxe comum. Essa sintaxe começa com as regras de JavaScript Object Notation (JSON). JSON descreve um objeto com pares de nome e valor que compõem o objeto. A gramática da política do IAM aproveita isso, definindo os nomes e valores, que têm significado e são compreendidos pelos serviços da AWS que usam políticas para conceder permissões.

O AWS Organizations usa um subconjunto de sintaxe e gramática do IAM. Para obter mais detalhes, consulte Sintaxe de SCP.

Erros de política comuns

- Mais de um objeto de política
- Mais de um elemento de declaração
- O documento da política excedeu o tamanho máximo

### Mais de um objeto de política

Uma SCP deve conter apenas um único objeto JSON. Você denota um objeto colocando chaves { } em torno. Embora você possa aninhar outros objetos dentro de um objeto JSON incorporando { } adicionais dentro do par de chaves externas, uma política pode conter apenas um par mais externo de { } chaves. O exemplo a seguir é incorreto, pois contém dois objetos no nível superior (destacados em *vermelho*):

```
{
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

No entanto, você pode atender a intenção do exemplo anterior com o uso de gramática correta da política. Em vez de incluir dois objetos de política completos, cada um com seu próprio elemento `Statement`, você pode combinar dois blocos em um único elemento `Statement`. O elemento `Statement` tem um conjunto de dois objetos como seu valor, como mostrado no exemplo a seguir:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Esse exemplo não pode ser mais compactado em um `Statement` com um elemento, porque os dois elementos têm diferentes efeitos. Em geral, você pode combinar instruções apenas quando os elementos `Effect` e `Resource` em cada instrução forem idênticos.

## Mais de um elemento de declaração

À primeira vista, esse erro pode parecer uma variação do erro na seção anterior. No entanto, sintaticamente é um tipo diferente de erro. No exemplo a seguir, há somente um objeto de política, como indicado por um único par de { } chaves no nível superior. No entanto, esse objeto contém dois elementos `Statement` dentro de si.

Uma SCP deve conter apenas um elemento `Statement`, que inclui o nome (`Statement`) que aparece à esquerda do sinal de dois pontos, seguido pelo valor à direita. O valor de um elemento `Statement` deve ser um objeto, denotado por chaves { }, contendo um elemento `Effect`, um elemento `Action` e um elemento `Resource`. O exemplo a seguir é incorreto, pois contém dois elementos `Statement` no objeto da política:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

Como um objeto de valor pode ser um conjunto de vários objetos de valor, você pode resolver esse problema combinando os dois elementos `Statement` em um único elemento com uma matriz de objetos, como mostrado no exemplo a seguir:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
```

```
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

O valor do elemento `Statement` é uma matriz de objetos. A matriz no exemplo consiste em dois objetos, sendo que cada um deles é um valor correto para um elemento `Statement`. Cada objeto na matriz é separado por vírgulas.

## O documento da política excedeu o tamanho máximo

O tamanho máximo de um documento de SCP é de 5.120 caracteres. Este tamanho máximo inclui todos os caracteres, também os espaços em branco. Para reduzir o tamanho da SCP, você poderá remover todos os caracteres de espaço em branco (como espaços e quebras de linha) que estão fora das aspas.

# Chamar a API por meio de solicitações de consulta HTTP

Esta seção contém informações gerais sobre o uso da API de consulta do AWS Organizations. Para obter detalhes sobre as operações e os erros da API, consulte Referência da API do AWS Organizations.

> **Note**
>
> Em vez de fazer chamadas diretas para a API de consulta do AWS Organizations, você pode usar um dos SDKs da AWS. Os SDKs da AWS consistem em bibliotecas e no código de exemplo para várias linguagens de programação e plataformas (Java, Ruby, .NET, iOS, Android e muito mais). Os SDKs constituem uma forma conveniente de criar acesso programático para o AWS Organizations e a AWS. Por exemplo, os SDKs processam tarefas como assinatura criptográfica de solicitações, gerenciamento de erros e novas tentativas automáticas de solicitações. Para obter informações sobre os SDKs AWS, incluindo como fazer download e instalá-los, consulte Ferramentas da Amazon Web Services.

A API de consulta do AWS Organizations permite chamar ações de serviço. As solicitações da API de consulta são solicitações HTTPS que devem conter um parâmetro `Action` para indicar a ação a ser realizada. O AWS Organizations oferece suporte a solicitações GET e POST para todas as operações. Ou seja, a API não requer 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. Embora esse limite dependa do navegador, um limite típico é 2048 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 na Referência da API do AWS Organizations.

Tópicos

# Endpoints

O AWS Organizations tem um endpoint individual de API global que está hospedado na região Leste dos EUA (Norte da Virgínia).

Para obter mais informações sobre AWS endpoints e regiões para todos os serviços, consulte Endpoints regionais no. Referência geral da AWS

# HTTPS obrigatório

Como a API de consulta retorna informações confidenciais, como credenciais de segurança, você deve usar HTTPS para criptografar todas as solicitações de API.

# Assinar solicitações de API do AWS Organizations

As solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta. É altamente recomendável não usar as credenciais da Usuário raiz da conta da AWS nas tarefas do dia a dia com o AWS Organizations. Em vez disso, use as credenciais de um usuário ou perfil do IAM.

Para assinar suas solicitações de API, você deve usar a AWS Signature versão 4. Para obter informações sobre como usar o Signature versão 4, consulte Assinatura de solicitações de API da AWS no Guia do usuário do IAM.

O AWS Organizations não dá suporte a versões anteriores, como Signature versão 2.

Para ver mais informações, 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 recursos da AWS, incluindo aqueles no AWS Organizations.
- Credenciais de segurança temporárias no IAM: descreve como criar e usar credenciais de segurança temporárias.

# Histórico da documentação do AWS Organizations

A tabela a seguir descreve as principais atualizações da documentação do AWS Organizations.

- Versão da API: 28/11/2016

| Alteração | Descrição | Data |
| --- | --- | --- |
| Declarações de política atualizadas | Foram adicionados novos `Sid` elementos às declarações de políticas AWS Organizations gerenciadas. | 6 de fevereiro de 2024 |
| Novo tópico sobre contas de gerenciamento de encerramento | Foram adicionados links para considerações e etapas detalhadas que explicam como fechar uma conta de gerenciamento. | 1 de fevereiro de 2024 |
| Práticas recomendadas atualizadas | Novas informações foram adicionadas à seção de práticas recomendadas para ajudar no alinhamento às práticas recomendadas do IAM. | 12 de junho de 2023 |
| Políticas AWSOrganizationsReadOnlyAccess atualizadas AWSOrganizationsFullAccess e gerenciadas | Ambas as políticas gerenciadas foram atualizadas visando permitir o acesso de gravação ou leitura a contatos para as contas. | 21 de outubro de 2022 |
| Atualizou a política AWSOrganizationsFullAccess gerenciada | A política gerenciada foi atualizada para permitir a criação de uma organização adicionando a permissão requerida para criar a função | 24 de agosto de 2022 |

| | | |
|---|---|---|
| | vinculada ao serviço de que uma nova organização precisa. | |
| Capacidade do Organizations de encerrar uma conta no console do AWS Organizations | As entidades principais na conta de gerenciamento podem encerrar contas de membros no console do AWS Organizations e usar políticas do IAM para proteger as contas de membros contra o encerramento acidental. | 29 de março de 2022 |
| Atualização do anúncio para atualizar contatos alternativos com o console do AWS Organizations | Você pode atualizar contatos alternativos para contas dentro de sua organização usando o console do AWS Organizations. Anuncie novos recursos e pontos para a Referência de gerenciamento de contas para obter instruções. | 8 de fevereiro de 2022 |
| Atualizações de política gerenciada pelo Organizations: atualização em uma política existente | As políticas foram AWSOrganizationsReadOnlyAccess atualizadas AWSOrganizationsFullAccess e gerenciadas para permitir as permissões de API da conta necessárias para atualizar ou visualizar contatos alternativos da conta por meio do AWS Organizations console. | 7 de fevereiro de 2022 |

| | | |
|---|---|---|
| Integração de Organizations com o Amazon DevOps Guru | Você pode integrar o Amazon DevOps Guru AWS Organizations para monitorar a integridade do aplicativo de forma holística em todas as contas da sua organização e obter insights. | 3 de janeiro de 2022 |
| Integração do Organizations com o Amazon Detective | Você pode integrar o Amazon Detective ao AWS Organizations para garantir que o gráfico de comportamento do Detective forneça visibilidade da atividade de todas as contas da sua organização. | 16 de dezembro de 2021 |
| A integração do Organizations com o AWS Config agora suporta a agregação de dados de várias regiões e várias contas. | Você pode usar uma conta de administrador delegado para agregar dados de configuração e compatibilidade de recursos de todas as contas-membro de sua organização. Para obter mais informações, consulte Agregação de dados de várias contas e regiõesno Guia do desenvolvedor do AWS Config. | 16 de junho de 2021 |
| Agora, a integração do Organizations com o AWS Firewall Manager inclui suporte para um administrador delegado | Agora você pode designar uma conta-membro de sua organização como administrador do Firewall Manager para toda a organização. Isso permite uma melhor separação das permissões da conta de gerenciamento da organização. | 30 de abril de 2021 |

| | | |
|---|---|---|
| Agora, as políticas de backup do Organizations são compatíveis com backup contínuo | Você pode usar o recurso de backups contínuos do AWS Backup com as políticas de backup de sua organização. | 10 de março de 2021 |
| Agora, a integração do Organizations com o AWS CloudFormation StackSets inclui suporte para um administrador delegado | Agora você pode designar uma conta de membro em sua organização para ser a AWS CloudFormation StackSets administradora de toda a organização. Isso permite uma melhor separação das permissões da conta de gerenciamento da organizaç ão. | 18 de fevereiro de 2021 |
| Continuar convidando contas enquanto você habilita todos os recursos | A AWS atualizou o processo para habilitar todos os recursos em uma organizaç ão. Agora você pode continuar convidando novas contas para ingressar em sua organizaç ão enquanto espera que as contas existentes respondam aos convites. | 3 de fevereiro de 2021 |
| Apresenta a versão 2.0 do console do AWS Organizat ions | A AWS apresentou uma nova versão do console do AWS. Toda a documentação foi atualizada para refletir a nova maneira de executar as tarefas. | 21 de janeiro de 2021 |

| | | |
|---|---|---|
| O Organizations agora suporta a integração com o AWS Marketplace | Agora é possível habilitar o AWS Marketplace para compartilhar com mais facilidade suas licenças de software com todas as contas de sua organização. | 3 de dezembro de 2020 |
| O Organizations agora suporta a integração com o Amazon S3 Lens | O Amazon S3 Lens suporta acesso confiável e administrador delegado com o Organizations. Para obter os detalhes, consulte Amazon S3 Storage Lens no Guia do usuário do Amazon Simple Storage Service. | 18 de novembro de 2020 |
| Cópias de backup de todas as contas | Quando são usadas políticas de backup para fazer backup dos recursos de sua organização, você agora pode armazenar as cópias de backup em outras Contas da AWS da organização. | 18 de novembro de 2020 |
| Agora, o Regiões da AWS na China é compatível com o AWS Resource Access Manager como um serviço confiável do Organizations | Agora é possível usar os recursos do AWS RAM que se integram com o Organizations como um serviço confiável quando você usa o Organizations e o AWS RAM na China. | 18 de novembro de 2020 |

| | | |
|---|---|---|
| O Organizations agora suporta a integração com o AWS Security Hub | Você pode habilitar o Security Hub em todas as contas de sua organização e designar uma das contas-membro de sua organização como a conta de administrador delegado para o Security Hub. | 12 de novembro de 2020 |
| Renomeada a conta mestra | O AWS Organizations alterou o nome da “conta mestra” para “conta de gerenciam ento”. Essa é uma alteração de nome apenas, não houve nenhuma alteração na funcionalidade. | 20 de outubro de 2020 |
| Nova seção e tópicos sobre Práticas recomendadas | Adicionada uma nova seção sobre práticas recomenda das para o AWS Organizat ions. A nova seção inclui tópicos que discutem as práticas recomendadas para o gerenciamento de usuários-raízes e senhas da conta de gerenciamento e das contas-membro. | 6 de outubro de 2020 |

| | | |
|---|---|---|
| Adicionada nova seção de práticas recomendadas e duas primeiras páginas | Há uma nova seção para tópicos que descrevem as práticas recomendadas para o AWS Organizations. Esta atualização inclui um tópico sobre práticas recomendadas para a conta de gerenciamento de uma organização e um tópico para práticas recomendadas para as contas-membro. | 2 de outubro de 2020 |
| Agora, as políticas de backup do Organizations são compatíveis com backups consistentes entre aplicativos em instâncias do Windows EC2 usando o VSS (Volume Shadow Copy Service) | As políticas de backup suportam uma nova seção `advanced_backup_settings `. A primeira entrada nesta nova seção é uma configuração de `ec2` denominada `WindowsVSS` , que você pode habilitar ou desabilitar. Para obter detalhes, consulte Criação de um backup do Windows habilitado para VSS no Guia do desenvolvedor do AWS Backup. | 24 de setembro de 2020 |

| | | |
|---|---|---|
| Organizations oferece suporte tag-on-create e controle de acesso baseado em tags | Você pode adicionar tags aos recursos do Organizations ao criá-los. Você pode usar políticas de tag para padronizar o uso de tags nos recursos do Organizations. Você pode usar as políticas do IAM para restringir o acesso apenas aos recursos que tenham chaves e valores de tag especificados. | 15 de setembro de 2020 |
| Adição de AWS Health como um serviço confiável | Você pode agregar eventos do AWS Health em todas as contas de sua organização. | 4 de agosto de 2020 |
| Políticas de exclusão de serviços de inteligência artificial (IA) | Você pode usar políticas de exclusão de serviços de IA para controlar se os serviços de IA da AWS podem armazenar e usar o conteúdo de clientes processado por esses serviços (conteúdo de IA) para o desenvolvimento e melhoria contínua dos serviços e tecnologias de IA da AWS. | 8 de julho de 2020 |
| Adição de políticas de backup e integração com o AWS Backup | Você pode usar as políticas de backup para criar e aplicar as políticas de backup a todas as contas de sua organização. | 24 de junho de 2020 |
| Compatibilidade com administração delegada para o IAM Access Analyzer | Permite delegar acesso administrativo para o Access Analyzer em sua organização a uma conta-membro designada. | 30 de março de 2020 |

| | | |
|---|---|---|
| Integração com AWS CloudFormation StackSets | Você pode criar um conjunto de pilhas gerenciado pelo serviço para implantar instâncias de pilha em contas gerenciadas pelo AWS Organizations. | 11 de fevereiro de 2020 |
| Integração com o Compute Optimizer | O Compute Optimizer foi adicionado como um serviço que pode funcionar com as contas de sua organização. | 4 de fevereiro de 2020 |
| Políticas de tag | Você pode usar política de tag para ajudar a padronizar tags entre recursos nas contas da organização. | 26 de novembro de 2019 |
| Integração com o Systems Manager | Você pode sincronizar dados de operações em todas as Contas da AWS em sua organização no Systems Manager Explorer. | 26 de novembro de 2019 |
| leis: PrincipalOrgPaths | Nova chave de condição global verifica o caminho do AWS Organizations para o usuário do IAM, a função do IAM ou o usuário-raiz da Conta da AWS que está fazendo a solicitação. | 20 de novembro de 2019 |
| Integração com regras do AWS Config | Você pode usar as operações de API do AWS Config para gerenciar as regras do AWS Config em todas as Contas da AWS de sua organização. | 8 de julho de 2019 |

| | | |
|---|---|---|
| Novo serviço para acesso confiável | O Service Quotas foi adicionado como um serviço que pode funcionar com as contas em sua organização. | 24 de junho de 2019 |
| Integração com o AWS Control Tower | O AWS Control Tower foi adicionado como um serviço que pode funcionar com as contas em sua organização. | 24 de junho de 2019 |
| Integração com AWS Identity and Access Management | O IAM fornece os dados do serviço acessado mais recentemente para as entidades de sua organizaç ão (raiz, UOs e contas da organização). Você pode usar esses dados para restringir o acesso apenas aos serviços da AWS necessários. | 20 de junho de 2019 |
| Marcação de contas | Você pode marcar e desmarcar contas na sua organização e visualizar tags em uma conta na sua organização. | 6 de junho de 2019 |
| Os recursos, condições e o elemento `NotAction` nas políticas de controle de serviço (SCPs) | Agora você pode especific ar recursos, condições e o elemento `NotAction` em SCPs para negar acesso entre contas em sua organização ou unidade organizacional (UO). | 25 de março de 2019 |

| | | |
|---|---|---|
| Novos serviços para acesso confiável | O AWS License Manager e o Service Catalog foram adicionados como um serviço que pode funcionar com as contas em sua organização. | 21 de dezembro de 2018 |
| Novos serviços para acesso confiável | O AWS CloudTrail e o AWS RAM foram adicionados como um serviço que pode funcionar com as contas em sua organização. | 4 de dezembro de 2018 |
| Novo serviço para acesso confiável | O AWS Directory Service foi adicionado como um serviço que pode funcionar com as contas em sua organização. | 25 de setembro de 2018 |
| Verificação do endereço de e-mail | Você deve verificar se possui o endereço de e-mail associado à conta de gerenciamento para poder convidar contas existentes para a sua organização. | 20 de setembro de 2018 |
| CreateAccount notificações | `CreateAccount` as notificações são publicadas nos CloudTrail registros da conta de gerenciamento. | 28 de junho de 2018 |
| Novo serviço para acesso confiável | O AWS Artifact foi adicionado como um serviço que pode funcionar com as contas em sua organização. | 20 de junho de 2018 |

| | | |
|---|---|---|
| Novos serviços para acesso confiável | O AWS Config e o AWS Firewall Manager foram adicionados como um serviço que pode funcionar com as contas em sua organização. | 18 de abril de 2018 |
| Acesso ao serviço confiável | Agora você pode habilitar ou desabilitar o acesso para que alguns serviços da AWS funcionem nas contas em sua organização. O IAM Identity Center é o serviço confiável inicial compatível. | 29 de março de 2018 |
| Agora, a remoção da conta é por autoatendimento | Você já pode remover contas que foram criadas no AWS Organizations sem entrar em contato com o AWS Support. | 19 de dezembro de 2017 |
| Adicionado suporte para novo serviço AWS IAM Identity Center | O AWS Organizations oferece suporte à integração com o AWS IAM Identity Center (IAM Identity Center). | 7 de dezembro de 2017 |
| A AWS adicionou uma função vinculada ao serviço para todas as contas da organização | Uma função vinculada a serviço denominada `AWSServiceRoleForOrganizations` é adicionada a todas as contas de uma organização para habilitar a integração entre o AWS Organizations e outros serviços da AWS. | 11 de outubro de 2017 |

| | | |
|---|---|---|
| Agora, você pode remover contas criadas | Os clientes já podem remover contas criadas em sua organização, com a ajuda do AWS Support. | 15 de junho de 2017 |
| Inicialização do serviço | Versão inicial da documenta ção do AWS Organizations que acompanha o lançamento do novo serviço. | 17 de fevereiro de 2017 |

# Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.